PORTFOLIO

Deep dives into topics that matter to community banks

Illustration by Creative Light/Adobe

“AI at the ATM extends that [bank-customer] relationship into a self-service channel that has historically been pretty impersonal.”

—SCOTT ANCHIN, ICBA

More vendors are integrating AI into ATMs. See what that means for community banks and their customers on page 25.

FOCUS SECURITY

Keep the gates shut against Trojan horse attacks

Community banks face cybersecurity risks from third-party vendors, which can serve as entry points for hackers. Here's what banks need to know about these threats and how to prevent them. By Jen A. Miller

Community banks have diligently fortified their organizations' walls against a range of cybersecurity attacks, but it's not going to matter if they don't know what their trusted partners could be letting in.

That's because despite the strong cybersecurity safeguards of community banks, third-party vendors can open avenues of attack if their security is not also up to snuff.

Threat actors are "looking for the path of least resistance," says Rob Farling, risk and compliance banking lead at business and technology consultancy West Monroe in Chicago. "What is an easier way to get that bank customer's money and information? There's a decent chance it's through the vendors."

Here's what community bankers need to know about spotting and stopping these Trojan horse-style attacks.

The threat landscape coming from third-party vendors has changed because banks' relationships, and volume of relationships, has changed by moving beyond relying solely on core providers for all technology needs, says Tom Wojcinski, partner in the cybersecurity and technology management practice at Wipfli, a consultancy based in Milwaukee.

Digital transformation, which has often involved expansion into the cloud and partnering with fintechs on new products, has meant that community banks can innovate, be nimbler and offer better services to their customers.

Illustration by Profit_image/Adobe

"[Threat actors are] looking for the path of least resistance. What is an easier way to get that bank customer's money and information? There's a decent chance it's through the vendors."

—ROB FARLING, WEST MONROE

But these changes have also increased potential attack vectors. According to Verizon's 2025 Data Breach Investigations Report, 30% of the 12,195 confirmed data breaches came from third-party vendors—double that of 2024.

Hackers target third-party vendors because they might not be as secure as banks have made themselves. With a successful third-party vendor hack, criminals wouldn't need to break into the bank. Instead, a vendor is already "[inside] the walls," says Farling. That means so is the threat actor who can steal information, plant malware or set the stage for a ransomware attack.

Categorize and assess vendor risk

Not every vendor will create the same kind of Trojan horse risk. There's a difference, for example, between a vendor having a point-to-point, permanent connection between itself and the bank, and a vendor that requires "periodic [connectivity] where you're just uploading information into their system or downloading into your system," says Wojcinski.

Community banks should stratify which vendors present different levels of risk and focus on the vendors that have the greatest access to the bank's internal systems or that store its most critical information.

While a bank can't completely protect itself against an attack on a third-party vendor, it can work to "minimize the risk" with different layers of protection, making sure any intrusion causes as little damage as possible, says Wojcinski.

One tactic includes limiting what a vendor can access inside a bank instead of giving it a constant connection that it doesn't need.

Community banks can also look at what data the vendor has and "how are we protecting that?" Wojcinski says. "Do we encrypt it before we send it? Is it in an encrypted [channel]? When a [vendor] sees it, how do they encrypt it, and how far does it stay encrypted in their system?"

When negotiating with new vendors or re-upping contracts, community banks can also make sure their agreement includes "what this software is going to do and what data [it] is going to have and where it is going to be stored," says Andrew Hettick, information security officer at data security firm CoNetrix, which is based in Lubbock, Texas. "If a vendor does have a breach, you would know exactly what data they have and where it would be vulnerable."

Community banks should also be aware of how long a vendor has to notify them of a breach. They should try to shorten that period for critical partners that have access to the most systems and data, he adds.

QUICK STAT

30%

of confirmed data breaches in 2025 came from third-party vendors, double that of 2024.

Source: Verizon 2025 Data Breach Investigations Report

Use cybersecurity basics to prevent a third-party heist

Potential threats coming in via third parties are a growing type of cybersecurity risk, but the attack types themselves and a bank's responses are not.

For example, if a vendor provides a service that is critical to a bank's functions, the bank should game out what it would do if that vendor was taken entirely offline by an attack. If a bank uses one vendor for all its loans, "and [the vendor is] ransomed and taken offline for three weeks, what's your fallback plan?" asks Wojcinski. Running tabletop exercises that include this type of scenario can help a bank prepare for an attack that might not get far enough to touch its systems but could still affect daily operations.

Vendors should also have multifactor authentication in place and use complex passwords or password managers for those logins, says Tim Rawlins, director and senior advisor at the NCC Group, a global cybersecurity company based in Chicago. And banks need to ask and not just assume vendors do. After all,

when the Louvre was robbed in 2025, the password to the museum's video surveillance system was "Louvre."

Communication is key to strong defense. Rawlins recommends that bank executives talk to not just the chief information officer and chief information security officer but also rank-and-file IT and security employees. All input about what they are experiencing and the challenges they face when working with third-party vendors are useful.

Executives might be surprised at what they hear. Sometimes, the bank might be the security problem, rather than the vendor. This can happen if the vendor must use an older, less-secure version of software because it's the only thing that will work with the bank's system.

"The people inside are going to know we should have upgraded," Rawlins says, "but we just haven't been given the budget to do it."

Review vendor security postures often

Assessing a vendor's security stance is almost always part of contract negotiations and renewals. A bank's cybersecurity insurance might also require that its vendors meet specific cybersecurity benchmarks.

But that can't be the only time a bank evaluates its vendors' security posture, says Farling. For low-risk vendors, a yearly check is probably enough. But for high-risk vendors—those that have access to the most sensitive data—banks should take a "continuous approach to monitoring assessment, more than the annual questionnaires," says Farling. "The risk is too great."

Closing these third-party vendor gaps is critical, he adds, not just for the health of the bank and potential compliance and regulatory blowback, but also for the bank's reputation.

Illustration by Dreamer82/Adobe

Be alert for impersonation schemes

Trojan horse attacks don't always start with hackers breaking into a bank via a third party. Sometimes, they pretend to be those vendors, says Tom Wojcinski, partner in the cybersecurity and technology management practice at Wipfli. For example, the 2023 ransomware attack on the British Library, which disrupted library operations for months, came through a hacker group that most likely used spear phishing to impersonate an IT vendor.

In 2024, a hacker successfully impersonated an approved vendor for the city of Baltimore. They stole $1.5 million by changing the real vendor's bank accounts in Workday, the cloud-based human resources and financial management platform, and taking the payments intended for the actual vendor.

Training employees to spot phishing attacks often focuses on hackers who are pretending to be coworkers to trick someone into giving away information or money, but it should include looking for this kind of spoofing, too.

Even if the fault lies with a third-party vendor, the bank is going to shoulder the blame.

"If you're going to open an account and have a bank hold your money, your assets, your life savings, you are operating under the assumption that the bank is protecting your assets," says Farling. A cyberattack, no matter where it comes from, "can erode that trust."

Jen A. Miller is a writer in New Jersey.

Illustration by NIA/Adobe

Leveling up fraud mitigation

By Wayne Miller, ICBA

When asked why he robbed banks, notorious 1930s-era bank robber Willie Sutton famously replied, "Because that's where the money is." While his response was purposely tongue-in-cheek, stopping criminals is a reality community banks face daily.

For as long as banks have been in existence, fraudsters have been targeting them. Today, a complicated mix of attacks that range from old-school check washing to AI-based deepfake scams and everything in between plague our defenses. It's not just whack-a-mole defense; it's manning multiple fronts. Community banks must address analog fraud while defending against new digital threats—a tall order no matter how you look at it.

Fortunately, community banks are in a state of constant vigilance, so fraud mitigation has become second nature. From historical safeguards like Positive Pay to new solutions like advanced anomaly detection, community banks execute fraud mitigation strategies using all the tools in their toolboxes.

From reactive to proactive

These resources now include solutions that help community banks move from a reactive to a proactive stance in addressing fraud. For instance, ICBA ThinkTECH Accelerator alum Socratix AI enables community banks to build secure, enterprise-grade AI agents that help fraud and risk teams investigate alerts in real-time and deliver structured insights. Meanwhile, Sardine, another ThinkTECH Accelerator participant, monitors thousands of signals to predict the likelihood of a scam in progress, resulting in more robust fraud detection protocols.

Another ThinkTECH Accelerator graduate, Overwatch Data, offers dark web monitoring to alert community banks to compromised card and check numbers, helping to prevent fraud campaigns, data breaches and cyberattacks before they affect customers or staff. And because so much of what takes place today is on cell phones, we can use tools that identify behavior that seems out of sync with normal activities.

ICBA support

I share these solutions with you not to push certain products but to raise awareness of the growing number of resources available to your bank. As fast as the fraud landscape is evolving, so, too, are the solutions that will help stop it in its tracks.

ICBA Innovation is here to support your fraud mitigation efforts. In every cycle, the ThinkTECH Accelerator selection and advisory committee seeks out the latest technologies that support fraud prevention and mitigation, because fraud is a constant consideration for all bankers.

We encourage you to engage with us as we launch our next cohort on May 18. Join other bankers in attending the Accelerator and hear from the companies that will be part of the next generation of fraud solutions. While we can't eliminate fraud completely, we can minimize its impact. And with new technologies at our disposal, we're poised to be stronger than ever.

Wayne Miller (*wayne.miller@icba.org*) is executive vice president and chief innovation officer for ICBA.

Next: Build a strong small business card program

FOCUS OPERATIONS

The biggest legal risks facing community banks

Between new technology and regulations, community bankers are understandably concerned about legal liability. We spoke with several lawyers about the types of lawsuits community banks should be aware of and how to prepare for them. By Don Sadler

Banks today are facing litigation risks on multiple fronts. This makes it critical to be aware of how plaintiffs' attorneys are using these legal theories to bring lawsuits against banks and what community bankers can do to protect their financial institutions from legal liability.

Overdraft and NSF fee cases

Abigail Lyle, partner with Hunton Andrews Kurth LLP, says there are a handful of very aggressive plaintiffs' attorneys who are focusing on overdraft and non-sufficient funds (NSF) fee cases.

"They are getting plaintiffs to sign a financial records authorization, which is sent to the bank requesting bank records on the client's behalf," she explains. "Then they mine this data to see if there's anything they can use to bring a lawsuit."

One common legal theory is what's referred to as "authorize positive, settle negative." In this scenario, funds are available when the transaction is authorized but insufficient by the time it settles due to intervening account activity. Plaintiffs claim that this is an unfair and deceptive practice if not adequately disclosed by banks.

Some core providers have created settings that allow banks to trace transactions to identify there were sufficient funds upon authorization even if there weren't at settlement and adjust the fee setting for those scenarios.

"So now, some attorneys are looking for banks that haven't implemented these settings or whose disclosures around such fees [could be viewed as] inadequate," says Lyle.

In a similar type of lawsuit, some plaintiffs challenge the use of the available balance without adequate disclosures around this practice. For example, some plaintiffs allege that the use of the available balance (which, unlike the ledger balance, often includes pending or hold items) results in the assessment of overdraft fees, even though the customer may have had a sufficient ledger balance to cover transactions when they posted. Plaintiffs have attempted to challenge this practice if there are not adequate disclosures as to the bank's balance methodology, including how and when such fees are assessed.

Lyle also points to lawsuits where plaintiffs allege that banks have assessed multiple NSF fees on the same returned item without adequate disclosure around the practice.

"For example, a merchant might re-present an item for payment that is rejected again if funds are still insufficient, and the customer is charged another NSF fee," she says. "It's critical to make sure there are adequate disclosures around how your bank will handle this practice."

Image by IRPAN/Adobe

Regulation E: Customer opt-in and consent

Another lawsuit community banks need to guard against involves customers consenting to being assessed overdraft fees under Regulation E. This regulation requires banks to provide a reasonable opportunity for customers to affirmatively consent and opt into covered overdraft services, along with a written or electronic notice describing the bank's overdraft services prior to opting in.

According to Lyle, some plaintiffs are claiming that the Regulation E opt-in form used by banks fails to provide a clear description of how and when overdraft fees will be assessed.

"For example, they claim that the form doesn't explain which balance method is used for determining if an account is overdrawn, or whether the fee is assessed at authorization or settlement," she says. "Therefore, they allege that any fees assessed using the form should be refunded to the customer."

Instead of immediately filing lawsuits, Lyle says many plaintiffs' attorneys are sending demand letters to try to get banks to settle confidentially, so the bank can avoid a public lawsuit. The best defense is a comprehensive review of all the bank's overdraft and NSF practices.

"It's not that you can't charge these fees," says Lyle. "You just need to make sure adequate disclosures are in place to clearly explain them to customers."

More from ICBA

Have more questions about legal liability? ICBA Education offers a range of on-demand seminars on current legal risks. *icba.org/education*

"[Attorneys] mine [client bank account] data to see if there's anything they can use to bring a lawsuit."

—ABIGAIL LYLE, HUNTON ANDREWS KURTH LLP

Cybercrime and data security

Cyber threats and data breaches are two other areas where community banks face rising litigation risks.

"These [cyber] lawsuits revolve around how banks handle sensitive information and protect against data intrusion by threat actors such as nation-states, organized cybercrime rings and hacktivists," says John Delionado, managing partner with Hunton Andrews Kurth LLP.

Threat actors are targeting customers' personal information (PI), banks' intellectual property (IP) and confidential business information, source code repositories and cloud environments. Recent data breach trends include ransomware, cyber extortion, business email compromise, doxxing and distributed denial-of-service attacks.

According to Delionado, every state has data breach notification laws that require banks to notify affected individuals if unencrypted PI is reasonably believed to have been accessed without authorization. In the event of a data breach, banks should determine if the compromised data is legally considered to be PI, when and how notification is required and whether an exemption applies.

Community banks' use of technology to track and record customers' interactions with their websites and online ads is another potential legal liability.

"There's a whole cottage industry of lawsuits and demand letters around this," says Delionado. These lawsuits claim that "cookies," the use of AI technology, such as chatbots, and other tracking technology like "pixels" are being used to send customer data to third parties without adequate disclosures and consent.

Last June, a federal court dismissed without prejudice a complaint alleging that a bank used pixels to collect and transmit website visitors' information to Facebook without proper notice of consent. However, many complaints have survived motions to dismiss.

"The best way to guard against claims like this is to find out if [the website or] anyone at your bank, including your marketing department, is using this kind of tracking technology," says Delionado. "If they are, carefully review your disclosures to make sure this use is covered."

Don Sadler is a writer in Georgia.

FOCUS PAYMENTS

How to compete in the small business card space

Community banks already have great relationships with small businesses. Offering tailored credit card programs is a way to further strengthen the community bank role as a trusted financial partner. By Colleen Morrison

Lake Ridge Bank in Middleton, Wisconsin, can customize credit cards for its small business customers.

Photo (hand) by Valiantsin/Adobe

Small businesses are increasingly reliant on credit cards, signaling an opportunity for community banks to build business. Sixty-two percent of small businesses report using a credit card on a regular basis, and nearly 29% sought a new credit card over the course of a year, according to the most recent findings from the Federal Reserve Banks' Small Business Credit Survey.

"Credit cards are an unsecured loan," says Kari Neckel, vice president of payments and technology policy at ICBA. "There is no easier way for a small business to spend the loan than with a business credit card issued from the community bank."

Identifying the right card program model

Credit card programs require thoughtful orchestration. At the highest level, community banks must decide if they want full programmatic control, and with it the internal risks and liabilities. Or they might prefer to lean more heavily on a partner to mitigate risk and support operational requirements.

Consider Lake Ridge Bank in Middleton, Wisconsin. The $3.1 billion-asset community bank owns and services its own credit card program, giving it complete strategic oversight and maximum flexibility to evolve its offerings as needed.

"A full banking relationship is one of our mantras, and our card program offers an opportunity for us to [expand] that relationship beyond the loan and the deposit functions at the bank," explains Scott Ducke, executive vice president and chief operating officer at Lake Ridge Bank. "I sit on the loan committee, and it's great to be able to say, 'Hey, we can approve you right here on the spot as you're moving your relationship over. We'll also approve you for X dollars in credit card availability.'"

Ducke notes that by having the program in-house, the bank can control risk to some extent by employing its knowledge of its clients.

"We've already got that banking relationship," he says. "[The program is] a perfect tool to mitigate that risk because we know our clients, and we know where their loans and their deposits are."

Seeking support from a partner

Other community banks appreciate being able to lean on a partner provider when running a card program. That's because when approvals, underwriting, correspondence, collections and support are handled in-house, they draw on internal resources and require additional oversight to ensure a safe, secure and successful program.

Citizens Bank of Las Cruces in Las Cruces, New Mexico, recently transitioned from an in-house program to a program supported by ICBA Payments and TCM Bank for those very reasons. Through this change, the $1.15 billion-asset community bank streamlined internal processes while launching a more competitive offering.

"Handling credit cards in-house was challenging, as it was not allowing us to be as competitive as we could have been in the banking industry," says Rhena Leitermann, senior vice president of treasury management and marketing at Citizens Bank of Las Cruces. "Now, we have three cards available to businesses that are specific to their needs, so they have flexibility on choosing what makes the most sense for them."

QUICK STAT

58%

of small businesses report using a credit card on a regular basis.

Source: Federal Reserve Banks' 2024 Small Business Credit Survey

"[Small business credit cards are] a perfect tool to mitigate that risk because we know our clients, and we know where their loans and their deposits are."

—SCOTT DUCKE, LAKE RIDGE BANK

Supporting small business needs with card programs

Small businesses depend on their cards. Data from Quickbooks shows credit cards serve as the number one solution for addressing cash flow problems.

"A credit card gives a business six to eight weeks between purchase and payment, and when the balance is paid in full, that becomes interest-free working capital—something most small businesses rely on," says Neckel.

Small businesses are also looking for specialized services that allow them to conduct business more efficiently.

For instance, rewards enable them to reap benefits, detailed transaction data helps with tracking and budgeting, and expense management enhances oversight over employee expenditures.

"Small businesses like rewards, but they also like to have access to a platform that allows them to handle their employees' expenses, close and add new employee accounts, change contact information in real time, offer customized reporting and provide easy access to all employee statements," says Leitermann.

Customization also speaks to small businesses in that it allows for ways to showcase their brand. For example, Lake Ridge Bank offers cards that can be designed and tailored for each of its small business clients—an offering that has become a key selling point.

"We win a lot of relationships because of the custom cards," Ducke says. "We take one in new business meetings, and prospective [clients] say, 'I just want that card with my logo on it.' They're really proud about the card, instead of just using it as a tool to move dollars around for them."

While the aesthetics are a nice-to-have feature, above all, Ducke sees credit card programs as an extension of the client relationship.

"Being that community bank for all their needs is probably the biggest support I would have for having your own card portfolio," he says. "We can really be part of that transaction and part of that relationship, rather than outside of it."

Colleen Morrison is a writer in Maryland.

Challenge the process

By Lindsay LaNore, ICBA

Illustration by Lustre Art Group/Adobe

Change is occurring at dramatic speed, and customer expectations are accelerating. As a result, it's more important than ever to "challenge the process." But this isn't about reckless disruption. It's all about learning-driven change and leading smarter.

The idea of challenging the process isn't new. In fact, it was one of the "five practices of exemplary leadership" that Barry Posner and James Kouzes talked about in their 1987 book, *The Leadership Challenge*. They asked leaders to challenge how things are done, to meet adversity head-on and to take opportunities to lead their organizations to new places.

Today, more than ever, keeping this idea top of mind can help leaders and teams stay relevant. At its core, this practice is about learning and willingness to change the status quo—for the better.

All companies fall prey to the "we've always done it that way" risk. It's human nature to want to stay the course, because it's comfortable, safe and feels easier to keep things the way they are. But as leaders, we must push boundaries and stop assuming that current practices are the best practices.

Consider any manual process you have at the bank. It's reasonable to believe manual processes are safer because they are subject to human vigilance. Data shows that isn't necessarily true for everything. As a leader, it's incumbent upon you to identify error-prone or inefficient areas (such as manual spreadsheets, re-keying or version control issues) and explore new ways of achieving the same goal. It is important to note that challenging the process doesn't just mean embracing a new technology to make it happen; reimagining a process to add value, improve efficiency or solve problems is also innovation.

So, how can you build the concept of challenging the process into your bank's culture?

- **Treat mistakes as opportunities to learn,** rather than moments to blame.
- **Ask "why" a process is the way it is.** If your team doesn't have a good answer, push them toward new exploration.
- **Create space during team meetings to poke holes in existing processes.** Again, this is not about blame but instead invites the team to question, suggest and experiment. Talk about when the process has worked and when it hasn't. Let the team get granular. Look for patterns or themes.
- **Ask "what if?"** This phrase helps to identify flaws or opportunities in a process by asking hypothetical questions.
- **Look at other industries as examples of innovation.** Host a meeting and ask every team member to bring an example of a satisfying product or service they have experienced recently. Talk about why it worked for them.

Finally, be open to exploring new learning and diving into the process at your bank. For expanded learning, check out ICBA Education's new Innovation Workshop.

Lindsay LaNore (*lindsay.lanore@icba.org*) is senior executive vice president and chief learning and experience officer for ICBA.

FOCUS SECURITY

AI at the ATM: Risks and rewards

ATM vendors are using AI tools to help keep machines running and provide community banks with better customer data. But this modernization does not come without risks. By Katie Kuehner-Hebert

Photo (ATM) by Pabkov/Adobe

Artificial intelligence is being integrated across all bank functions—including within ATMs.

AI can help keep ATMs up and running, tailor the experience to individual customers and give banks better data about how the channel is being used, says Scott Anchin, ICBA's senior vice president of strategic initiatives and policy. For community banks, that kind of intelligence can level the playing field.

"Community banks have always had an edge when it comes to knowing their customers," he says. "AI at the ATM extends that relationship into a self-service channel that has historically been pretty impersonal. When the technology can adapt to how a customer actually uses the machine, it starts to feel less like a piece of hardware and more like an extension of the bank."

Preventing ATM failures

For technology and services provider Diebold Nixdorf, AI-driven predictive maintenance is essential to always-on ATM availability, says Jodi Neiding, vice president of global banking hardware solutions for the North Canton, Ohio-based company.

Diebold Nixdorf's DN AllConnect® Data Engine combines cloud connectivity, machine learning and AI to monitor device health, diagnose root causes and predict failures before they occur, Neiding says.

"This enables proactive service, resolving issues remotely or dispatching technicians with the right part, so banks can move from reactive repairs to self-healing operations," she says. "The result is higher uptime, fewer disruptions and a more reliable self-service experience for consumers."

Atlanta-based NCR Atleos is also modernizing ATM operations through an AI-assisted service platform they developed called Intelligent Diagnostics, which instantly analyzes fault data and provides prescriptive repair guidance with over 95% accuracy to reduce manual troubleshooting and improve first-time fix rates, according to Stuart Mackinnon, executive vice president and chief operating officer.

"AI overcomes the limitations of traditional predictive analytics by correlating multiple signals to forecast potential part failures and by optimizing technician dispatching to ensure the right resource arrives on the first visit, boosting availability and reducing repeat service calls," Mackinnon says.

These capabilities are already delivering measurable impact for the ATMs NCR Atleos services, including a 13% global reduction in service revisits and a 50% decrease in North America tech support cases, he says.

Enhancing customer experience

Mackinnon says AI helps transform ATMs into dynamic digital access points for customers by enabling natural voice interactions, full audio-guided experiences and seamless authentication via voice. AI-powered digital humans can also address staffing challenges by offering guided, relevant prompts that personalize the experience and support customers more effectively, he says.

AI is transforming ATMs into

intelligent, connected service points within a broader omnichannel ecosystem, Neiding says. Financial institutions are unifying digital, branch and self-service interactions through real-time data insights, personalization and seamless channel integration.

"AI can streamline routine transactions, anticipate customer preferences and enable expanded services such as video banking or account origination," she says. "Combined with capabilities like cash recycling and managed services, AI-powered tools like cash forecasting improve efficiency and availability while elevating the user experience."

Security risks and mitigation strategies

However, the same AI tools that are improving ATMs are giving criminals new capabilities, Anchin says. More sophisticated fraud attempts are occurring across every channel, and ATMs are no exception.

"Any time you're adding new technology and new connections to a device that handles financial transactions, you have to think carefully about what risks come along with that," he says.

To neutralize these risks, banks need to ask the right questions of their vendors, like what data is being collected, where it goes and how the AI is making decisions, Anchin says.

3 questions to ask vendors of AI-enabled ATMs

1. What data is being collected?
2. Where does that data go?
3. How is the AI making decisions?

Examiners are increasingly focused on how banks manage technology risk, and that includes understanding the tools that third-party providers—including ATM vendors—are putting on the bank's network.

"None of this should discourage community banks from exploring AI at the ATM, but you can't let the excitement outrun your risk management framework," Anchin says. "When criminals are using AI to attack, banks need to be ready to use AI to defend."

The key is doing it thoughtfully, with strong vendor due diligence and policies that keep pace with the technology, he says.

"The result [of AI-driven ATM predictive maintenance] is higher uptime, fewer disruptions and a more reliable self-service experience for consumers."

—JODI NEIDING, DIEBOLD NIXDORF

AI's risk-detection capabilities

Diebold Nixdorf's AI-enabled ATM systems can recognize transaction irregularities like jackpotting by analyzing historical data, including transaction rates and volume ratios, to identify suspicious patterns, Neiding says.

"AI strengthens protection, supporting real-time fraud detection, anomaly monitoring and faster incident response across ATM networks," she says. "These capabilities complement established safeguards such as anti-skimming technology, biometric authentication and secure cloud connectivity."

NCR Atleos' AI-powered video analytics can detect abnormal or malicious behavior in real time—such as a car backing toward an ATM, hand movements consistent with installing a skimmer or signs a customer may be under duress. This allows the system to trigger alarms or protective countermeasures proactively, Mackinnon says.

"AI in self-service banking doesn't introduce new risks so much as extend existing ones," he says. Banks have always managed concerns like data privacy, system reliability and fraud prevention, and AI simply adds new security layers—such as biometrics—to frameworks already in place.

"With proper safeguards, policies and leadership oversight, AI becomes an evolution of current digital strategies rather than a disruptive shift," Mackinnon adds. "The same principles used for any new banking technology still apply: transparency, fairness, strong governance and maintaining human oversight."

Katie Kuehner-Hebert is a writer in California.

FOCUS LENDING

How to help businesses through signs of distress

Community banks support customers in not just the good times but the bad ones, too. By fostering open communication and being proactive about addressing financial distress, banks can help businesses navigate these challenges and come out stronger. By Mindy Charski

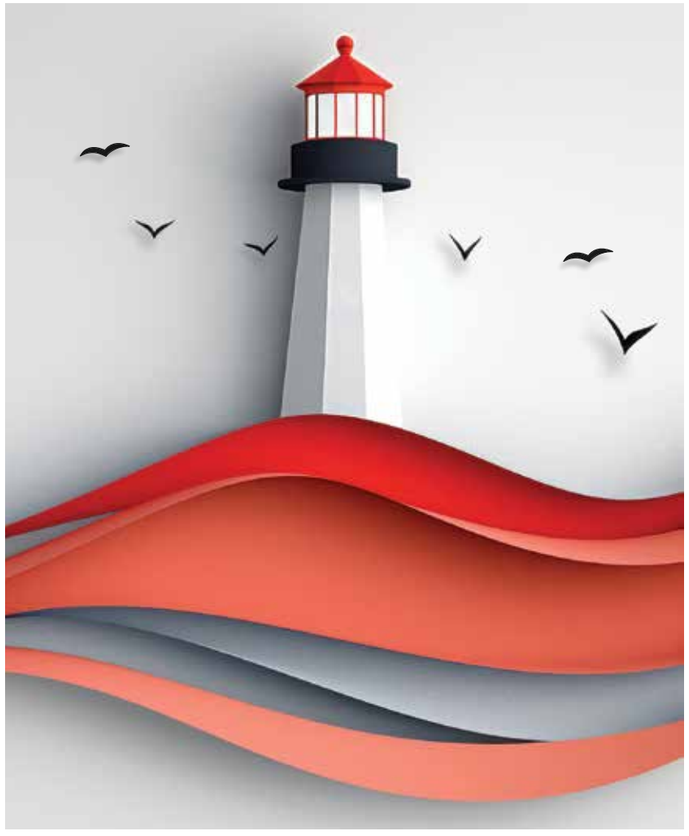

Illustration by Lustre Art Group/Adobe

During a routine annual financial review of a borrower's business, Kathryn Perry—SVP, chief lending officer and chief financial officer at $160 million-asset Park State Bank & Trust in Woodland Park, Colorado—noticed something alarming. While the customer had never had a late payment, she says she saw "extreme distress" in the cash flow of his equipment restoration company. He had taken high-interest loans from other lenders to keep his payments current, and she would later learn he was considering bankruptcy.

Her bank was able to help its customer of more than 15 years get back on track through solutions that included extending the loan's maturity, providing interest relief and arranging a new appraisal on his building, providing equity as a source of cash.

"It was surprising to me that, even at this stage in the relationship, he had not gotten the message: 'Trust your community bank. We want to see you succeed as much as you want to succeed,'" says Perry.

Relationship banking isn't just about helping customers in the good times. Community banks that put in the work to help borrowers facing difficulties can both stave off defaults and deepen customer loyalty.

Early warning signs

Maintaining good communication with customers can help banks stay in the loop about the status of a customer's business.

"I think it's all about being in touch with your customer, being in tune with your customer and not being transactional," says Joe Vereline, first vice president and director of business banking at $3.2 billion-asset Union Savings Bank in Danbury, Connecticut.

Perry works to build trust with new customers even before the first loan closes. She says Park State Bank & Trust encourages clients to call the bank first, not last, when trouble arises. But there are reasons customers at any bank might not be upfront about challenges they're facing. They might be too embarrassed, for instance, or scared the bank will add to their stress.

"For a small business customer, especially in a rural area, they often think of the bank as on the opposite side of the table, as in, 'The minute I start to have any trouble, I have to fear the bank rather than rely on the bank,'" Perry says.

Financial data can illuminate issues that go unmentioned. Data analytics tools are enabling bankers to get "better access to information, more timely information and information that's organized in a way that you can make decisions more quickly," says Gill Hundley, chief operating and risk officer at KlariVis, a performance intelligence platform for community banks and ICBA preferred service provider. "If you can get ahead of problems, then you can plan for them."

KlariVis' software extracts data from core banking systems each night, providing up-to-date information such as past dues, for both individual loans or aggregated loans in a specific industry. However, traditional methods are still effective at spotting potential turbulence before borrowers miss a loan payment.

Vereline says Union Savings Bank looks out for indicators in borrowers' annual financial reports such as shrinking profit margins, weakening cash flow, and declining top-line revenue, liquidity or collateral values. If an otherwise prompt customer delays submitting financial information, that can be a red flag.

Union Savings Bank also monitors borrowers' operating accounts for significant drops in average balances and deposits. The mutual bank also keeps up with trends in the industries of its loan customers to see if they're in decline or facing headwinds.

Mitigating issues

Community banks can take different approaches to help businesses showing signs of distress. Institutions can make an impact by acting as business advisors, what Perry describes as "analyzing their business and using our experience and expertise to help guide them." That could entail helping customers address overhead concerns, slumping sales or delays in receivables, for example.

If necessary, banks can address problem loans with options like deferring payment, refinancing or restructuring. Further down the road, they could require more collateral or obtain additional guarantors, Vereline says.

"We want to do what's right for the bank … but we also want to do what's right for the customer," he says. "So, where do we meet in the middle and find that common ground that works for both of us?"

A solid solution can be worth pursuing. Vereline says being the bank that restructures a loan or defers payments can be advantageous when the borrower's business is booming again.

"They're going to come to us when they need that next loan," he says. "They're going to hopefully remember that we were the ones that were there to help them out when times were tough."

Perry puts a finer point on it. "A $1 million or $2 million relationship with a small business for me, when I've only got $160 million in assets, is a huge relationship," she says. "I am far more motivated [than larger banks] to [help the business get stabilized] rather than to simply charge it off and move on."

Mindy Charski is a writer in Texas.

> **"It's all about being in touch with your customer, being in tune with your customer and not being transactional."**
>
> —JOE VERELINE, UNION SAVINGS BANK

QUICK STAT

96%

of small businesses say they faced at least one financial challenge in 2025.

Source: Federal Reserve Banks' 2026 Main Street Metrics survey

Next: ICBA asks Congress for more fraud support

In with the new

Introducing ICBA Securities' new endorsed broker-dealer.

By Jim Reber and Ryan Hayhurst, The Baker Group

Photo by Siti/Adobe

Jim Reber: Ryan, what a difference a couple of months makes. Last fall, ICBA Securities' board of directors asked management to study the depository fixed-income broker market and make a proposal for a relationship that would carry ICBA and its members into the future. From that, we identified The Baker Group as the first best option. The board agreed, and after a couple of months of negotiations, we sealed the deal in early March. Tell us about The Baker Group and your multi-decade career with one firm.

Ryan Hayhurst: The Baker Group was founded in 1979 by a community banker who saw a need for a firm that could help community banks manage their interest rate risk through investment portfolio management. Today, we have grown to one of the largest, independently owned, full-service broker-dealers serving community banks nationwide with a focus on education, asset-liability management and investment portfolio management.

Much like how our clients are community banks, I like to think of us as a "community broker-dealer" focused on the needs of the customers we serve rather than an out-of-state owner that only cares about the bottom line.

As for me, I joined The Baker Group in 1991 as a wet-behind-the-ears college intern, and I immediately fell in love with the people and culture that make up the Baker family. Thirty-five years later, I couldn't imagine ever working for another company.

Jim: Next, what can you tell us about Baker's interest in and response to ICBA's invitation to submit a proposal last year?

Ryan: We were thrilled when ICBA reached out and asked us to submit a proposal to become the newly endorsed broker-dealer for ICBA Securities. As you know, The Baker Group was a finalist back in 1988 when ICBA selected its first endorsed broker, and unfortunately, we came in second place.

But we didn't give up. We developed new and better tools, we expanded our education platform, doing 50 to 70 events a year, and we focused on what community banks needed. Thirty-seven years later, the opportunity came around again, and we jumped on the chance to submit a proposal.

Community banks are the lifeblood of America, and this endorsement will allow us to take our shared mission of serving and supporting community banks to an even bigger audience.

Jim: Many of our readers know there has been another twist to this ICBA Securities–Baker Group arrangement, which is that I joined the Baker team effective April 1.

I, too, have had a terrific run with one broker. I started as an ICBA Securities sales rep in 1992 and succeeded the legendary C.J. Pickering as president and CEO in 2005. ICBA was a fantastic employer, and I got the best of both worlds in my view: a position in the bond business where I've got some history (notoriety?), and continued collaboration with some of the best in the business among all three ICBA pillars: advocacy, innovation and education. So, there's a lot to be said for continuity. (And I'm working on the "we" and "they" pronouns as I transition, so be patient.)

Ryan: I can't tell you how excited we are to have you join the Baker team. Your experience, reputation and integrity are unparalleled in this industry. In fact, once the announcement was made that we would become the new endorsed broker for ICBA Securities, the very first question every banker and state association asked me was, "Is Jim Reber coming to Baker?" I am proud to say, "Yes!"

Jim: We should also tell our readers they'll be seeing some changes to this Portfolio Management column. One of the many reasons Baker was invited to contract with ICBA is its deep bench of strategists and speakers. What are your plans for *Independent Banker*, and what can you tell us about Baker's commitment to community bank bond education?

Ryan: Education is one of our pillars, along with investment portfolio and asset-liability management. We remain committed to continuing our long history of providing in-person and virtual education programs designed specifically for community banks.

As for this column, we plan to continue your legacy of providing valuable (and entertaining!) investment insight, but through a range of contributors. You'll be hearing from not only me but also several other members of our Financial Strategies Group.

Jim: Let's not forget about Baker's capacity to partner with ICBA's state affiliates, which was a matter of high rank in the selection process.

Ryan: That's right. We understand just how important state banking associations are to community banks. We are bringing endorsements from ICBA state affiliates in Illinois, Texas, Indiana and Alabama into the mix, so we know what it takes to work with these associations as they fight for community banks in their state. We have partnered with state banking associations for more than four decades to provide industry-leading education and financial support, and we look forward to working with all 34 state associations that endorse ICBA Securities.

Jim: Very good. I am honored that The Baker Group offered me this position, and I intend to remain visible to ICBA members and attend conventions whenever practicable. In the near term, my objective is to get Baker integrated into the ICBA extended family as efficiently as possible. I'm beyond excited about this new chapter for ICBA Securities and The Baker Group.

Ryan: I couldn't agree more, Jim. Welcome aboard!

> **"I like to think of us as a 'community broker-dealer' focused on the needs of the customers we serve rather than an out-of-state owner that only cares about the bottom line."**
>
> —RYAN HAYHURST, THE BAKER GROUP

Jim Reber, CPA, CFA (*jreber@gobaker.com*) is managing director of ICBA relations at The Baker Group.

Ryan Hayhurst (*ryan@gobaker.com*) is president of The Baker Group, ICBA Securities' endorsed broker-dealer.

Fraud doesn't stop at the bank door

Community banks can't solve the problem of fraud on their own. See what ICBA is doing to address financial fraud and how community bankers can advocate for fraud prevention on Capitol Hill.

By Amber Milenkevich and Scott Anchin

Illustration by Rafagat Batool/Adobe

Bank fraud isn't going away. It keeps changing and getting harder to manage as AI-driven scams, check fraud, account takeovers and other financial crimes hit banks from multiple angles.

Last year, 60% of financial institutions and fintechs surveyed by Alloy saw an increase in fraud compared with 2024, with organized crime rings responsible for 71% of those incidents.

Community banks deal with this every day. Testifying before the House Financial Services Committee's Subcommittee on Financial Institutions, Gay G. Dempsey, CEO of Bank of Lincoln County in Fayetteville, Tennessee, described fraud as a constant issue that keeps shifting and getting harder to manage.

In her testimony, Dempsey talked about the many types of fraud banks are dealing with right now, from romance and impostor scams that start on social media to checks stolen and altered before they ever hit an account. The damage doesn't stop with the individual customer either, she said. It reaches small businesses and local communities and has real consequences for the people community banks serve.

"Escalating fraud losses are a priority concern for community banks," Dempsey said. "I have dedicated considerable time and effort to fighting payments fraud and scams, having witnessed first-hand the impact on my customers, my bank and peer community banks, local small businesses and our community. Fraud creates financial ruin for too many individuals and endangers local prosperity."

What's on the agenda

ICBA is calling for changes that would give community banks more time and flexibility to stop fraud before losses build, including:

- Longer hold times and clearer guidance under Regulation CC so banks have time to catch suspicious deposits
- A dispute process that helps banks quickly pursue check fraud claims
- Keeping Federal Reserve check services that help identify and stop fraud
- Supporting the STOP Fraud Act and the Bank Fraud Technology Advancement Act, both of which would give banks better tools to deal with evolving fraud threats

Through our Fraud and Scams Task Force, ICBA has developed guidance on check fraud liability, detection methods and how to escalate disputes when another bank is involved. That guidance is built around real cases and day-to-day issues and backed by training that helps staff recognize and address the threats. The task force brings together people across roles, from CEOs to operations teams to fraud investigators, to meet regularly, compare notes, share what they're seeing and work through possible responses.

Regulators have also joined those discussions, giving community banks a direct way to share feedback and push for changes based on what's happening in the field.

No sector can solve this alone

ICBA also supports the SCAM Act (H.R. 7548), which would require online platforms to take more responsibility for fraudulent and deceptive ads and strengthen enforcement of consumer protection laws. Many of the scams Dempsey described in her testimony begin there, forcing banks to limit the damage after the fact.

We've also been raising awareness of the unique challenges community banks face on both the regulatory and legislative fronts. They operate close to their customers and know firsthand how these scams play out in real time. Our members also operate with fewer resources and tighter constraints than larger institutions. That combination shapes how they respond and what they can realistically do to stop fraud before losses occur. Having a community banker speak about those experiences in a public hearing helps policymakers understand those realities.

ICBA also understands that banks don't operate in a vacuum. They might wind up absorbing the fallout from scams that started somewhere else, like on a social media platform or through a spoofed phone call. Dempsey laid both out in her testimony and in the questions she fielded at the hearing. She made the case that getting a handle on fraud requires buy-in from stakeholders well outside the banking world.

Bottom line? No single sector can solve this alone, and the answer can't stop at the bank door.

> **ICBA … supports the SCAM Act (H.R. 7548), which would require online platforms to take more responsibility for fraudulent and deceptive ads and strengthen enforcement of consumer protection laws.**

QUICK STAT

60%

of financial institutions and fintechs saw an increase in fraud in 2025 compared with 2024.

Source: Alloy

Resources at your disposal

ICBA has resources in place that members can start using right now to manage the evolving fraud environment. The Fraud and Scams Task Force is open to new members, for example, and includes people across roles, from CEOs to fraud investigators. The group meets regularly to share what members are seeing and work through responses together.

The fraud channel on ICBA Community is another option that members get involved with. More than 1,000 members use it to share intelligence, cases and strategies. You can participate as actively or passively as you'd like, but either way, you'll have access to what your peers are dealing with and how they're responding.

On the legislative front, if you have meetings scheduled with members of Congress, ask them to cosponsor the SCAM Act. It's an important ask that reflects what community banks are seeing firsthand and dealing with daily.

Amber Milenkevich is ICBA vice president of congressional relations.

Scott Anchin (*scott.anchin@icba.org*) is ICBA senior vice president of strategic initiatives and policy.