

The 2026 ProSight State of Fraud Prevention Survey

Escalating Threats and
Evolving Defenses

Contents

About ProSight 3

About the Survey and Report..... 4

Survey Findings at a Glance..... 5

Part I: The Alarming Threat Environment..... 7

 The Big Picture: ‘Under Assault at Scale’ 7

 The State of the AI-Enabled Fraud Battle 9

 Real-Time Payments: Instant ... and Irrevocable 11

 Account Takeovers Prompt Proactive Safeguards 13

 APP Scams Highlight the Transition to Fraud Prevention 13

 Check Fraud: The Problem That Won’t Fade Away..... 14

 The Fraud-Fighting Budget: Spending More Is Only Part of the Solution 16

Part II: Room for Improvement..... 18

 The Time for Better Industry Cooperation Has Come 18

 Education Can Help Customers Help Themselves 21

 Employee Education Can Strengthen the Last Line of Defense..... 22

Closing Thoughts..... 23

About ProSight

ProSight Financial Association empowers financial services leaders to strengthen and advance our industry. Formed through the merger of BAI and RMA—trusted organizations with rich histories and deep expertise in risk, fraud, compliance, and retail and commercial banking—we provide connections, training, insights, tools, and analytics to help you act with confidence. Our work creates positive ripple effects throughout financial services organizations and the industry, generating new opportunities for growth and ultimately helping consumers, businesses, and communities thrive. Learn more at ProSightFA.org.

Acknowledgments

The 2026 ProSight State of Fraud Prevention Survey: Escalating Threats and Evolving Defenses is published by ProSight Financial Association. ProSight developed the research hypotheses and analyzed the research results. Celina Rogers, Sam Knox, and Frank Devlin directed the research and wrote the report. Janet Nowaczyk managed the project. Thank you to Isio Nelson and Jason Bartolacci of the ProSight Fraud Alert Network for their valuable contributions. A very special thank you to the industry leaders working in fraud prevention who participated in this research program. This work would not have been possible without you.

Please direct inquiries to Katie Williams at kwilliams@ProSightFA.org.

Design by Christopher Santoro.

October 2026

© 2026 ProSight Financial Association. All rights reserved, including the right to reproduce this report or portions thereof in any form whatsoever.

About the Survey and Report

ProSight Financial Association fielded its initial State of Fraud Prevention Survey in summer 2026. Bank and credit union leaders working in business lines, compliance, cybersecurity, finance, fraud prevention, information technology, legal, and risk were among the 125 banking professionals from institutions throughout North America who completed the survey.* The institutions they represent include credit unions and banks of all sizes, from small community institutions to global money center banks.

The research program, which included post-survey interviews with bankers and industry experts, highlighted the big picture strategies and the practical steps financial institutions are employing to address the persistent and growing problem of fraud.

* Throughout the report, percentages may not add up to 100 due to rounding.

Survey Findings at a Glance

Fraud continues to proliferate at an alarming pace—despite considerable investments to contain it. That’s no surprise to the bankers on the front lines and the millions who try to evade the traps set by wrongdoers daily. Nor to the Office of the Comptroller of the Currency (OCC): In its most recent Semiannual Risk Perspective for spring 2026, it called fraud “a key driver of operational losses,” saying “banks continue to face challenges from elevated levels and sophistication of fraud and scams.” The upsurge is becoming increasingly difficult for financial institutions to manage as old-school fraud flourishes at the same time AI and real-time payments create modern challenges. With one survey commenter describing an industry that is “under assault at scale,” 20% of respondents said fraud activity increased “substantially” in the past year, with 73% of all respondents saying fraud is growing. The pick-up in fraud’s pace is hitting particularly hard at institutions below \$10 billion in assets, where 32% said the increase has been substantial.

Operational—not financial—factors are the most common constraints in preventing fraud. Fifty-three percent of respondents said their institutions increased their fraud budgets by 5% or more this year, yet 85% said the fraud threat is growing faster than their ability to respond. Put simply, banks are spending more money on the fraud problem than ever before, but they’re still struggling to operationalize fraud prevention fast enough. Top operating barriers to fraud prevention efforts include alert overload, staffing limitations, data quality, and various IT limitations.

AI is benefitting fraudsters more than financial institutions. Banks and credit unions are increasingly deploying AI. In fact, the survey found that it

has substantially changed the way fraud is fought at over 20% of banks over \$10 billion, and at 10% of smaller institutions. Still, an overwhelming 87% of all respondents said AI is ramping up fraud—think AI-enhanced phishing, impersonation attacks, synthetic identities, deepfakes, and automated fraud campaigns—faster than fraud prevention. The question for banks has shifted quickly, from “Should we use AI?” to “Can we deploy AI fast enough to get ahead of bad actors?”

Real-time payments controls are a very real priority. As payment speeds accelerate, fraud detection has been forced to move from retrospective investigation to real-time intervention. Real-time monitoring and risk-based fraud controls (for example, adaptive multi-factor authentication) are increasingly important as fraud prevention moves from a back-office function to real-time automated flags and decisioning. Expanding real-time transaction monitoring and analysis was the most commonly cited (41%) fraud prevention priority over the next 12 to 24 months. Improving real-time payments controls was No. 4 on that list (25%).

Check fraud is the old-school exploit that endures. Despite the seismic shift to digital transactions prompted by the Covid pandemic, survey results reveal that fraud is decidedly not confined to online spaces. With banks and credit unions grappling with old-school fraud at the same time they try to safeguard digital spaces, survey respondents were more likely to cite check fraud as a top area of loss exposure (58%) and their fastest-growing fraud method (46%) than any other type.

Customer education and industry cooperation are promising areas where ground in the fraud fight can be gained. In an environment where scam-driven losses make customer awareness as or even more important than technical controls, banks are seeking to enlist customers as part of their overall fraud-defense system. Customer human error/judgment gaps was the leading category of preventable fraud losses named by respondents (62%). And the vast majority (87%) reported that their institutions plan to invest more in customer education. Meanwhile, several respondents said communication between institutions about threats is lacking, and nearly two-thirds said they’re very interested in deepening their collaboration and information sharing with peer institutions.

Part I: The Alarming Threat Environment

The Big Picture: ‘Under Assault at Scale’

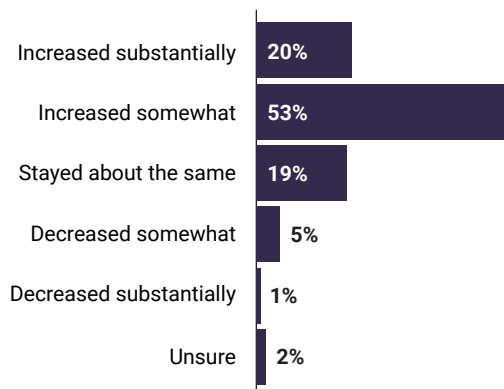
The fact that financial system fraud is proliferating is no surprise, but it is worth considering the extent to which this threat is growing. A full 20% of survey respondents said fraud affecting their institution has increased substantially in the past year (see Figure 1). Fifty-three percent said it has increased somewhat, and about 20% said it has stayed about the same. Only 6% said it has abated, with the rest unsure. The pick-up in fraud’s pace is hitting particularly hard at institutions below \$10 billion in assets, where 32% of respondents said the increase has been substantial, compared to 4% at banks in the \$10 billion to \$100 billion range and 13% at banks over \$100 billion. More than two-thirds of banks from the latter categories reported that the volume of fraud affecting their institution has increased in the past year.

In its most recent Semiannual Risk Perspective for spring 2026, the OCC said fraud is “a key driver of operational losses, and banks continue to face challenges from elevated levels and sophistication of fraud and scams.”

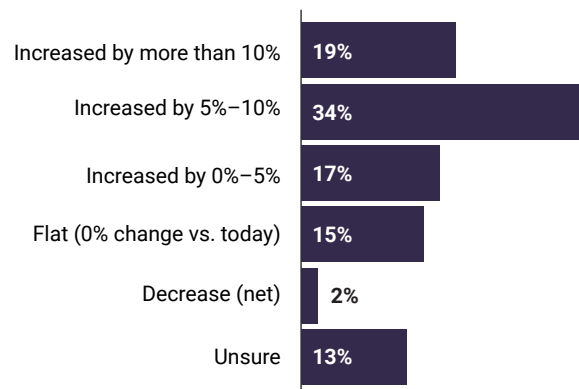
“Financial systems are under assault at scale,” a respondent from a community bank said in a written survey response. “Stopping [fraud] appears to be difficult and becoming more so. Attempts to stop [it] require excessive investment and even with education, customers make bad choices.”

Figure 1. Fraud activity and banks' anti-fraud spending are on the rise

Over the past 12 months, how has fraud volume affecting your institution changed?



How has your institution's budget for fraud prevention changed in its most recent fiscal year?



A BSA/AML officer at a community bank noted the dwindling efficacy of two-factor authentication, saying, “the bad actors know how to manipulate the account holders into providing that pin number.”

In a post-survey interview, Whitney Darcy, senior vice president, BSA and fraud operations manager at Fidelity Bank NA, a \$3 billion institution based in Wichita, Kansas, said financial institutions and consumers are challenged by a world where “people are inundated with text messages, phone calls, and social media messages that are all the start of a scam.”

This rise in fraud that’s being felt almost universally—from check fraud, to authorized push payment (APP) scams, to deepfakes and automated campaigns—may explain why so many respondents feel like they are falling behind in the battle. Eighty-five percent of respondents said the fraud threat environment is changing faster than they can respond, with 21% saying the environment is changing much faster. In other words, said Jason Bartolacci, director of ProSight’s Fraud Alert Network, “the bad guys are always a couple steps ahead of us,” adding “I am not hearing a lot of optimism right now.”

The State of the AI-Enabled Fraud Battle

AI is making it easier for fraudsters to succeed.

“The rate that AI is increasing fraud and making things look more realistic for people to click on” is not just an issue for “the normal everyday people” who are falling victim, said Susan Adamson, vice president of operational risk at Farm Credit Illinois, in a post-survey interview. “Sometimes it’s more difficult for me to know...is this an actual email?” she said.

Thirty-three percent of respondents said fraudsters are substantially ahead of financial institutions in the AI space as one side uses the technology to perpetrate crime and the other side seeks to prevent it (see Figure 2). Another 54% said fraudsters are somewhat ahead, while 10% said the adversaries are on equal footing. Only 3% said banks are ahead.

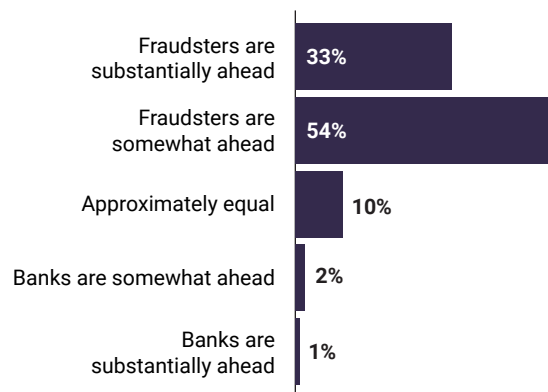
This is an area where institutions under \$10 billion feel particular stress. More than half (54%) said fraudsters were substantially ahead, with 41% saying fraudsters were somewhat ahead. That split was 24% substantially/41% somewhat for banks in the \$10 billion to \$100 billion range and 15% substantially/59% somewhat for larger banks.

“My biggest concern is that AI is making fraud more convincing and much easier to scale,” a C-level executive at a community bank said. “Identity verification and behavioral monitoring will become even more important over the next few years.”

“We have huge concerns and are investing in anti-AI fraud tools from a cyber and client perspective,” a compliance executive at a mid-tier bank said.

Figure 2. Fraudsters achieve the upper hand with AI

In your view, who is currently ahead in the use of AI for fraud and fraud prevention?



How is your institution proactively addressing fraudulent activities?



Note: “Unsure” responses were excluded from the data set; n=123.

Banks and credit unions are increasing spending on their own AI to level the playing field. In fact, 81% of survey takers—the largest response—said technology investment was a top way they are proactively addressing fraudulent activities. Sixty percent said technology spending, including for AI, has brought about a moderate change in how they address fraud, with 18% saying the change has been substantial. Here, institutions above \$10 billion were more likely to report substantial technology-fueled change, including 24% of respondents from institutions ranging from \$10 billion to \$100 billion in assets and 21% from larger banks. That compared to 10% from institutions below \$10 billion. Common applications include transaction monitoring, cited by 67% of respondents, and onboarding (52%). AI is also commonly used in risk scoring/modeling (43%), customer interaction/decisioning (32%), and case management/workflow (29%).

AI’s effectiveness at financial institutions is limited, however, by issues including data reliability (cited by 48% of respondents), talent/expertise (37%), technology integration (36%), and regulation/explainability (36%).

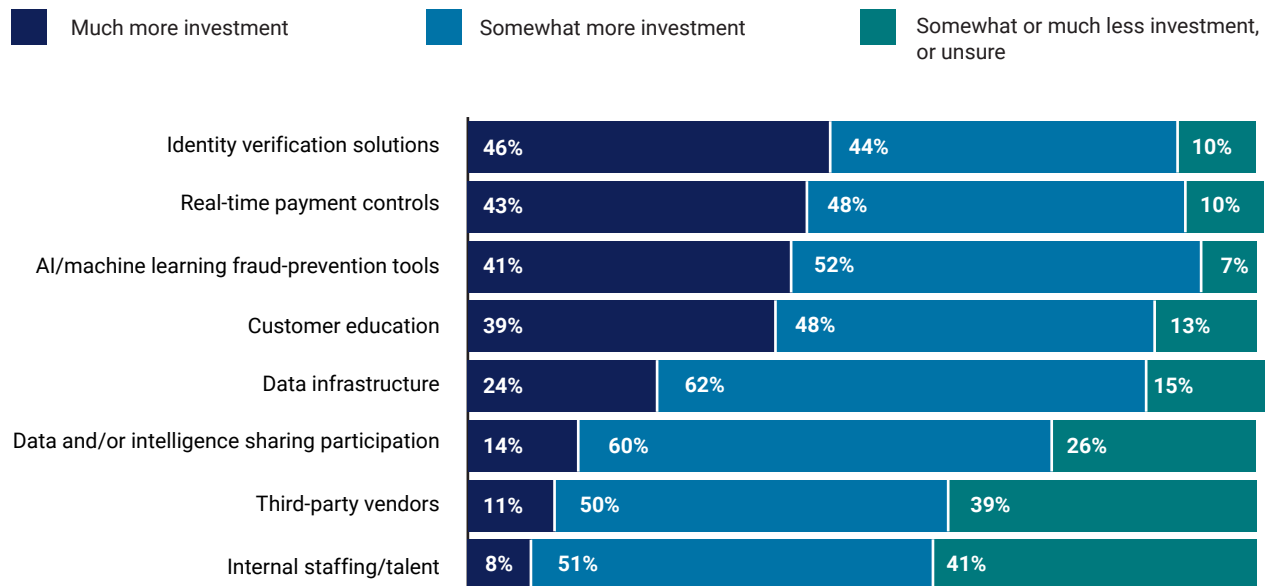
“Fraudsters do not need to comply with AI or model governance rules,” a senior risk executive at a community bank said. “They do not care if they have a 98% fail rate—2% is easy money, and the AI tools are cheap.”

Real-Time Payments: Instant ... and Irrevocable

Real-time payments ranked high on the list of respondents' concerns throughout various survey sections. Real-time payment controls were named as a likely area for future budget increases by 43% of respondents, second only to identity verification solutions (46%), as shown in Figure 3. Meanwhile, expanding real-time payments monitoring and analysis was the top fraud-prevention priority named (41%). Twenty percent of respondents said real-time rails including RTP, Zelle, and FedNow were among their greatest areas of loss exposure, and a quarter said real-time payments were among their three fastest-growing types of fraud.

Figure 3. Banks boost spending on ID verification, real-time payment controls, and AI-enabled fraud prevention technology

To what extent does your institution plan to increase fraud-related investment in the following areas over the next three years?



“With the quickness in which these payment types move, it is imperative to add additional layers of scrutiny before the funds leave the institution,” a BSA/AML officer at a community bank said.

“We are implementing additional controls and confirmation steps throughout the payment workflow to slow users down and encourage validation of payment details before submission,” an executive at a global money center bank said. “These measures help ensure clients verify the intended recipient and understand who they are sending funds to before initiating irrevocable real-time payments.”

A majority of respondents said they were taking the “better safe” route in the tension between a seamless customer experience and the friction that is often required to mitigate fraud. Half said they prioritize fraud mitigation, while 8% prioritize customer experience. Forty-one percent said they balance the two opposing goals equally.

“We are willing to add appropriate friction during the onboarding process because protecting our members and the security of their accounts is a top priority,” a credit union leader said. “Additional verification steps may create a small amount of inconvenience, but they help confirm member identities, reduce the risk of fraud, and prevent unauthorized access. We strive to balance a smooth member experience with strong safeguards that build trust and protect our financial community.”

A community bank executive noted a decidedly consumer unfriendly—but intentional—process in the drive to mitigate losses. “We have tightened ... debit card controls, such that a customer’s allowed transactions OFTEN get declined, as a result of a risk matrix that generates based on their card usage (places, apps, dollars, # of transactions, etc.).” The approach is not optimal, the executive said, but it is practical because “we are really limited with what we can do to mitigate losses both for us and our customer base.”

Account Takeovers Prompt Proactive Safeguards

Account takeover (ATO) fraud was ranked as a top-three loss exposure by 35% of respondents and one of the fastest-growing types of fraud by 37%. Respondents said they are fighting account takeovers with stricter verification controls for call center and contact information updates, improved detection and alert systems, more sophisticated anti-money laundering software, and restructured teams to reduce silos. A senior compliance executive at a mid-tier bank said a new behavioral biometric monitoring system at the institution provides “real-time alerting, monitoring, and intervention” to stop account takeovers.

A leader at a global money center bank, meanwhile, said, “We are reducing ATO risk by requiring stronger authentication controls, including mandatory MFA [multi-factor authentication]. We also implemented email domain validation to prevent changes to publicly available email domains, helping protect against unauthorized account access and account compromise.”

APP Scams Highlight the Transition to Fraud Prevention

APP scams/social engineering was an area of greatest loss exposure for 30% of respondents, and 40% said it was among the fastest growing fraud modes. Thirty-four percent said reducing scam/APP losses was among their top three fraud-prevention priorities over the next 24 months. This form of fraud is one example of how the banking industry is transitioning from a fraud-prevention approach focused on detecting unauthorized transactions to a model that includes fighting scams, social engineering, and AI-enabled fraud in real time. Bad actors hacking into accounts remain a major problem, but the growing risk, and perhaps the biggest risk, is criminals persuading customers to move their own money willingly. “We are observing the highest increase in fraudsters scamming customers into giving them their online credentials and bank imposters contacting customers that then give the fraudsters their PPI,” a community bank compliance executive said.

“With a compliance/BSA staff of just two it is extremely difficult to manage,” a community bank compliance executive said. “We rely heavily on [a third-party anti-fraud platform] and pour a lot of effort into educating staff and community, and partnering with departments in the bank like operations, IT, and finance, in real time, to ensure we cover as many bases as possible as quickly as possible for all events.”

Maria Noriega, product and community manager for ProSight’s Fraud Alert Network, said, “the proliferation of fraud means that even teams at large institutions can feel stretched thin. The fast pace and the increasing capability of fraudsters leave many teams in the position of trying to keep up and even triaging.”

Check Fraud: The Problem That Won’t Fade Away

While the Covid-era boom in digital transactions undoubtedly transformed the industry, fraud is hardly confined to the digital realm. The industry continues to grapple with the fraud of the past while simultaneously fighting modern fraud tied to real-time payments fraud and AI-enabled threats.

Check fraud—fueled by mail theft, check washing, counterfeiting, and altered checks—shows no sign of slowing. It was named more frequently than any other category as a top area of loss exposure. Fifty-eight percent of respondents cited it, ahead of other critical concerns like debit card fraud (37%), account takeover (35%), and authorized push payment scams/social engineering (30%), as shown in Figure 4.

Figure 4. Check fraud generates the greatest fraud exposure

Which of the following types of fraud create the greatest loss exposure at your institution today?



Check fraud was also the top answer (46%) when respondents were asked to name the fastest-growing type of fraud at their institution. At institutions under \$10 billion, 74% of respondents said it was a top area of loss exposure and 63% said it was among their fastest-growing fraud types.

“Check fraud is the largest fraud loss budget bucket,” Darcy of Fidelity Bank said in a post-survey interview. “And I allocate the largest portion of my fraud loss budget to take losses on altered counterfeit or forged checks.”

In written responses, other respondents said they were acting to mitigate this persistent scourge by implementing continuous frontline training, revising hold practices, enhancing transaction monitoring and ID verification, and urging customers to make payments electronically rather than by check.

One community bank's BSA/AML officer sounded a hopeful note about the institution's "new check-fraud monitoring system, which utilizes a review of the actual image to determine if the item might be fraudulent. [The] system auto clears items that are legitimate, helping save time to process the items that might be suspicious."

Such comments reflect the complexity of the check fraud battle, with both fraudsters and financial institutions applying modern technology to an age-old method of payment to boost their chances of success. "Banks have historically treated check fraud as a legacy payments problem, while criminals have turned it into a modern fraud ecosystem involving mail theft, mule accounts, counterfeit production, and digital deposit channels," said ProSight Managing Director of Research, Fraud, and Thought Leadership Isio Nelson. "In talking to executives at banks," Nelson said, "we've learned that one challenge they grapple with is justifying investing fraud-prevention dollars in a declining payment type—checks—when those investments are needed to defend the growing space of digital payments."

The Fraud-Fighting Budget: Spending More Is Only Part of the Solution

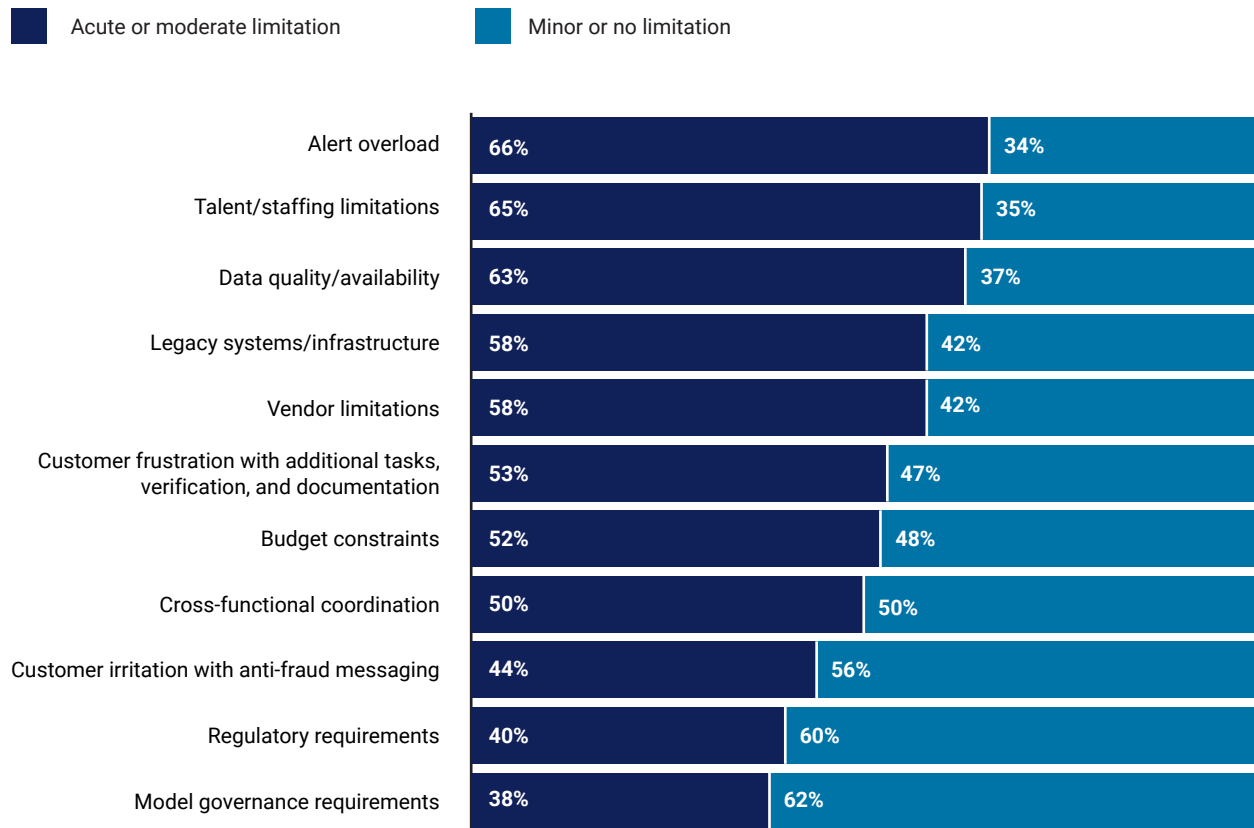
Budget constraints ranked in the bottom half of the factors limiting anti-fraud efforts, with 52% of respondents calling it an acute or moderate limitation (Figure 5). The top three answers were alert overload (66%), talent/staffing limitations (65%), and data quality/availability (63%), suggesting that operational—not financial—factors are the most common constraints in preventing fraud.

Legacy system infrastructure (58%), vendor limitations (58%), and customer frustration with additional tasks, verification, and documentation (53%) were also named more frequently than budget constraints.

Put simply, banks are spending more money on the fraud problem than ever before, but they're still struggling to operationalize fraud prevention fast enough.

Figure 5. Too many alerts, staff limitations, and data quality limit banks' effectiveness in fighting fraud

To what extent do the following factors limit your institution's anti-fraud programs and activities?



Note: "Unsure" responses were excluded from the data set; n=121.

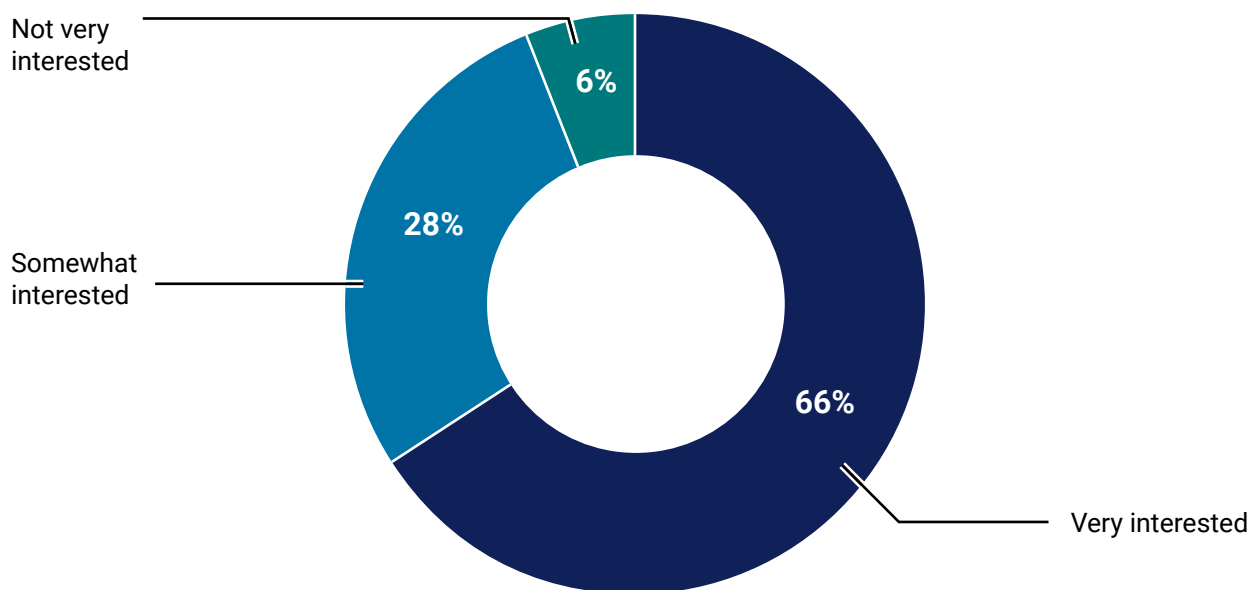
Part II: Room for Improvement

The Time for Better Industry Cooperation Has Come

Some good news, survey respondents said, is that amid a wave of advanced technological threats, some traditional philosophies and approaches could help to tamp down fraud's rise. One is the importance of cooperation and information-sharing among financial institutions. Only 24% of respondents say they share information about notable fraud incidents with peer institutions through informal channels, and even fewer (20%) share information through formal industry networks or platforms. Some respondents said other financial institutions do not respond promptly enough to their requests under 314(b), the section in the Patriot Act that provides the ability to share information under a safe harbor that offers protections from liability. Nonetheless, nearly two-thirds of respondents say they are very interested in deeper collaboration and information sharing with other institutions (see Figure 6).

Figure 6. Two out of three respondents are eager to swap fraud information with peer institutions

To what extent are you and your institution interested in deeper collaboration and information sharing among banks and other financial institutions on fraud detection and fraud risk management?



Note: "Unsure" responses were excluded from the data set; n=111.

A community bank executive said, "there needs to be more pressure for timely review of cases," while a compliance executive at a money center bank said, "real-time responses to 314(b) requests would go a long way" in combating fraud.

At the same time, survey results and respondent comments indicate that banks increasingly recognize that fraud is becoming a network problem, in addition to an institution-level and financial system one. Improved defenses may stem from shared intelligence rather than focusing on isolated detection and prevention models.

"The tone that is generated from media outlets and politicians is that banks are solely accountable for protecting clients from their own actions," a regional bank executive said. "The narrative hardly ever includes social media, telephone/mobile carrier, and client accountabilities to mitigate fraud. Additionally, the bad actors are hardly ever convicted. There [are] often no remarks about strengthening the criminal justice system. The tone

needs to shift to a collective responsibility instead of solely focusing on FIs as the culprit in failing to adequately defend against fraud.”

Fidelity’s Darcy spoke of the wins that can result from collaboration. She said she launched a Metro Area Fraud Investigators Association (MAFIA) group for her region that includes personnel from 21 other area financial institutions—plus 12 law enforcement agencies.

“We have over 75 people that we are able to share information with here in Wichita,” she said. “We’re able to quickly communicate ‘I just got hit with this type of scam’ or ‘this guy’s traveling around opening accounts.’”

The area group’s efforts are consistent with a broader regulatory and industry trend toward improving data sharing and collaboration as part of institutions’ overall fraud defense. In fact, the Financial Crimes Enforcement Network (FinCEN) just [issued updated guidance](#) in June to clarify how financial institutions can share information under 314(b).

ProSight has addressed the interest in collaboration by launching its aforementioned [Fraud Alert Network](#), which allows members to share intelligence, receive timely alerts, and coordinate fraud prevention efforts.

Other regulators have signaled an effort to address growing fraud in general. In June, the Federal Reserve, the OCC, and the FDIC announced a request for comment on “potential actions to help consumers, businesses, and financial institutions mitigate [the] risk of payments fraud, with a particular focus on check fraud.”

Eighty-eight percent of survey respondents expect the level of regulatory and examiner attention on fraud to increase over the next two years, with 22% saying they expect it to increase substantially. “The immediate thing that can be done from a regulatory standpoint is to promote the sharing of verified fraud data with peers,” an executive at a regional bank said.

Education Can Help Customers Help Themselves

Incidents related to customer error/judgment gaps were named as the most preventable fraud loss by 62% of ProSight survey respondents. The vast majority of respondents (87%) reported that their institutions plan to invest more in customer education, whether that means website information, reminders on statements, or special classes or chats in branches. Darcy said her team at Fidelity created a wallet card printed with fraud red flags for customers. Keeping it handy means that “if a situation seems weird, you’re not trying to dig for a website or pull out a booklet.” While her bank has long engaged in such efforts, she said, next year she will create a separate customer education line item for the anti-fraud budget.

In a written survey response, an executive from a regional bank said, “we are putting considerable effort into educating clients to not fall victim to phishing and smishing.”

“It’s like the movie ‘Jerry Maguire,’” another respondent said. “‘Help me help you.’ The more proactive clients are, they not only protect themselves, but they protect the bank and everyone else in the network.”

Most respondents said they are not concerned that their multiple and frequent messages beseeching customers to be on guard will land as annoying or, worse, blaming. Only 20% said they agreed with the statement: “We tone down our fraud education to avoid blaming customers, creating extra work for them, or undermining their confidence in our security.” Three-quarters of respondents disagreed, including 50% who did so strongly.

“The risk of upsetting the customer is low compared to the possible loss, both financially and reputationally if fraud occurs,” a community bank line of business leader said.

Employee Education Can Strengthen the Last Line of Defense

Employee human error/judgment gaps (named by 49% of responses) and branch processes such as insufficient verification (45%) were seen overall as the second- and third-most frequent causes of preventable losses.

Darcy said that every little bit that can be achieved in the way of additional employee education is worthwhile, even if it means finding time amid the varied schedule of a universal banker to review, say, the warning signs that a check could be fraudulent.

Adamson of Farm Credit Illinois said that such education remains one of the most effective investments a financial institution can make in fraud prevention. While technology and controls are important, she noted that frontline employees and relationship managers are often the last opportunity to identify suspicious activity before funds leave an account.

That education goes beyond teaching employees what to look for, she said. It helps build the confidence to ask difficult questions, challenge unusual transactions, and engage customers in meaningful conversations when something does not seem right. “It can be uncomfortable asking, ‘What are you doing with that money?’” Adamson said. “But when employees are equipped with the right training and understand the warning signs, they become the human in the loop, adding the judgment and critical thinking that technology alone cannot provide.” In many cases, she added, a well-trained employee can be the difference between a successful fraud attempt and a prevented loss.

Closing Thoughts

The findings of the 2026 ProSight State of Fraud Prevention Survey paint a challenging picture: fraud is growing in both volume and sophistication, fueled by the convergence of persistent legacy threats such as check fraud and rapidly evolving risks tied to AI, social engineering, and real-time payments. Financial institutions are investing more in technology, increasing budgets, and strengthening controls, yet many still feel the threats are moving faster than their ability to respond.

At the same time, the survey points to glimmers of hope that the proliferation of fraud can be turned back. Respondents consistently highlighted opportunities to improve outcomes through a combination of human and technological defenses. Advanced analytics, AI-driven monitoring, and real-time risk controls can help institutions detect and stop fraud more effectively. Equally important are the people behind those tools: educated customers, well-trained frontline employees, stronger information sharing among institutions, and closer collaboration with regulators and law enforcement.

Financial institutions are investing, modernizing, and collaborating at unprecedented levels to combat fraud. They are adopting advanced technologies, increasing funding, strengthening controls, and building stronger partnerships across the industry. Yet despite this progress, many leaders remain concerned that fraudsters are innovating even faster, leveraging new tools, techniques, and attacks at a pace that challenges traditional defenses. The race between fraud prevention and fraud innovation has never been more intense, making continued investment, agility, and collaboration essential to staying ahead of an increasingly adaptive threat.



Fraud moves at machine speed. AI redefines fraud threats and prevention.

Get ahead of AI-accelerated fraud and modernize your fraud prevention strategies with the ProSight Fraud Alert Network community.

AI is compressing the time between attack and impact. Twenty-seven seconds is one of the fastest eCrime breakout times on record in 2026.*

Connecting experts. Sharing knowledge. Mitigating fraud.

Join the ProSight Fraud Alert Network

Complimentary for ProSight members for one year

*2026 CrowdStrike Global Threat Report: AI Accelerated Adversaries

