AMERICAN BANKER

Partner insights from REFINE INTELLIGENCE

WHITEPAPER

Stop Scams Before They Strike

Smarter data and real-time context empower banks to detect and block fraud as it happens.

Scams are evolving faster than ever before, in large part, thanks to AI and other digital technologies. Today's scammers can work a variety of cons at scale, whether defrauding elders, luring people into fake romance schemes or peddling phony investments. The dramatic increase in the volume and sophistication of scams has banks and credit unions looking for any available tools to stem the tide, from consumer education and staff training to new digital technologies that help detect potential scams.

In September of 2025, Arizent, parent company of American Banker, in partnership with Refine Intelligence, surveyed 114 banking professionals about scams and how their institutions are responding to the surge in fraud. The results show financial institutions feel like they are falling short on scam prevention, but most have yet to hit on an effective solution that doesn't rely too heavily on customer vigilance or resources institutions can't afford to deploy.

Scams represent a major risk to financial institutions and their customers

The number and variety of scams confronting consumers and businesses has grown substantially in recent months. That growth has raised the overall threat level around the world and created significant financial harm. Large majorities of financial institutions say that during the past year they have seen an increase in the volume of scams (76%), monetary volume of customer losses (70%) and bank losses (63%).

Scams also generate a variety of significant impacts beyond financial losses. Financial institutions need to detect, investigate and recover from the damage caused by these schemes. Roughly two-thirds (67%) cite operational costs related to investigation time, staffing and case handling as the biggest impact of handling scam claims. Smaller institutions feel this impact even more acutely — 80% of banks with less than $5 billion in assets cite operational cost as a significant impact on their business.

Additional impacts include costs related to recovering funds and managing customer relationships. More than half of respondents (55%) cite tracing funds and reimbursing customers (55%) as top concerns. Almost half (47%) cite reputational damage or erosion of customer trust as a major impact. Larger institutions are particularly concerned about reputational damage (70%), as they tend to be subject to stronger media scrutiny and higher customer expectations for sophisticated safeguards.

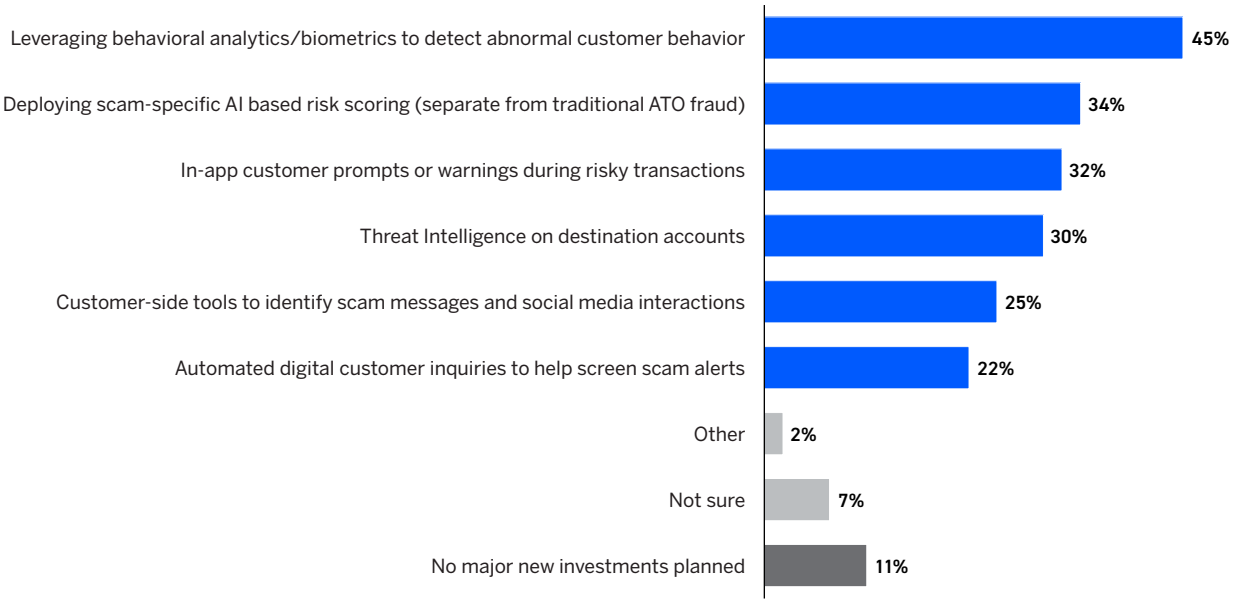
Financial institutions are looking for more effective ways to prevent scams

Consumers are ill-equipped to protect themselves, particularly as fraud volume increases and scams appear in more varied forms. Because they often lack knowledge about how to protect themselves and have fewer safeguards and systems in place than businesses, scammers consider them attractive targets. Nearly four in five financial institutions (77%) say that the volume of scams targeting consumers has increased the most during the past year compared to just 18% that have seen more of an uptick in scams targeting businesses (for example, business email compromise).

A lack of awareness also often means victims don't recognize scams as they occur. Financial institutions cite consumer education and awareness (40%) as the biggest barrier to scam prevention, followed by the growing sophistication of the scams themselves (34%). If banks can't get a handle on education and awareness, the increasing sophistication of scams will only become a bigger threat.

Efforts to educate customers about scams frequently fall short of their goal. Virtually all financial institutions (91%) believe that there are gaps in their scam controls versus the desired situation. In response, banks plan to invest in a wide range of technologies to help them combat fraud. Nearly nine in 10 financial institutions (86%) say there is strong executive support for significant investments in fighting scams. The question is where that investment should be directed, since no organization sees a silver-bullet technology that will eliminate the problem on its own (see Figure 1).

Figure 1: Banks recognize that there is no single technology that will solve the scam problem



Source: Arizent/American Banker 2025

Organizations are pursuing a variety of solutions, both on the back end (behavioral biometrics and AI-based risk scoring) and customer-facing (in-app prompts and tools that help identify scam messages and social media interactions). Larger banks are particularly interested in AI-driven solutions that prompt customers for more information during risky transactions. More than half of the largest banks (55%) plan to increase their investment in AI solutions over the coming year. That compares with just 16% of smaller banks.

Notably, a quarter of small banks say they plan no major investment in anti-scam technology of any kind. This inactive stance potentially leaves their customers vulnerable as the fraud threat grows. That effect could snowball as the lack of investment and the resulting exposure it creates can erode customer trust and, ultimately, the bank's ability to compete.

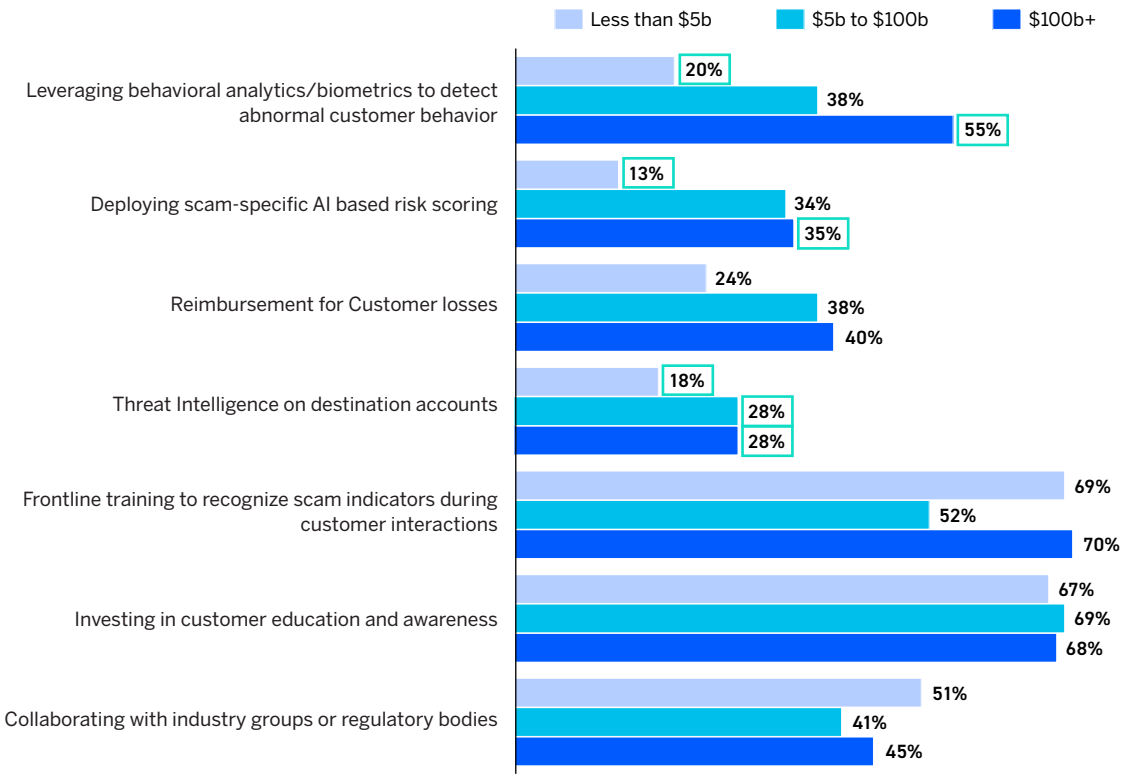
For a bank to maintain trust, it must prove that it can both identify scams and help keep customers safe through consistent, sustainable anti-scam processes. "Identifying a potential scam is only the first step in keeping customers safe," says Uri Rivner, CEO and Co-founder of Refine Intelligence. "The next question is, how do we quickly, effectively resolve the alert? Whether done by analysts or AI, additional context is needed to arm the institution with accurate powerful insight—and the best way to get it is asking the customers themselves, preferably at scale while creating a positive customer experience."

> **"Identifying a potential scam is only the first step in keeping customers safe. The next question is, how do we quickly, effectively resolve the alert?"**
>
> — **Uri Rivner**,
> CEO and Co-founder
> Refine Intelligence

Small banks risk falling behind on scam prevention

Larger banks have generally been more aggressive in adopting controls to identify or prevent customer scams (see Figure 2).

Figure 2: There are significant gaps between large and small banks' scam-prevention controls



Green boxes indicate statistically significant differences between highest and lowest values in the group at a 95% CI
Source: Arizent/American Banker 2025

Only 20% of small US financial institutions with less than $5 billion in assets have adopted advanced anti-scam practices such as behavioral analytics and biometrics, far fewer than banks with more than $100 billion in assets (55%). Small institutions also lag larger ones in the use of scam-specific AI-based risk scoring (13% versus 35%), as well as reimbursement for customer losses (24% versus 40%).

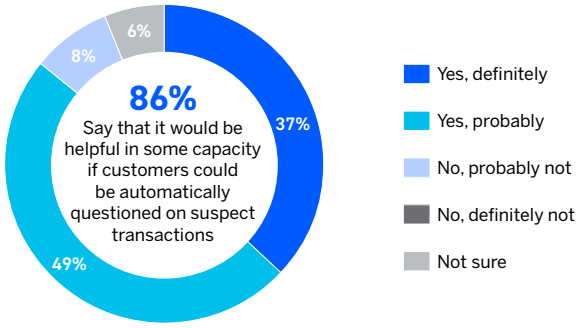
Smaller banks have invested roughly equally with larger banks in frontline training, education and awareness. They're also generally more likely to collaborate with industry groups or regulatory bodies than larger institutions.

Reliable context about a customer's activity can improve scam detection and prevention

When fighting scams, human analysts and AI often lack crucial context. AI tools can easily flag unusual transactions, but they cannot identify them as fraudulent without additional information, such as the nature of the customer's activity and their relationship with the beneficiary. For example, it might not be immediately clear if someone is giving a gift to a friend or losing money in a scam.

For human analysts, determining context is costly, impractical and difficult. Even with specialized training, human analysts may find it difficult to promptly get the information necessary for a deep analysis of any individual transaction. This is an area in which automation could change the game (see Figure 3).

Figure 3: Almost all bank professionals believe that automated customer outreach would help



Source: Arizent/American Banker 2025

Digital solutions can help financial institutions solicit the context they need from the people best able to provide it: the customers themselves. Some tools can automatically contact a customer in real time to obtain information about a suspicious transaction. The most streamlined solutions use follow-up questions tailored for specific situations that are vulnerable to scams, such as gifts, investments and bill payment.

By leveraging user interaction and transactional data, this technology can even determine when a customer is misleading the bank in an attempt to make a scam transaction go through, for example if a scammer is guiding the customer how to answer. Monitoring the time required to answer a simple question, an inability to provide specific answers and other tripwires can help spot scams while they're in progress. Tools capable of this level of sophistication allow financial institutions to cut through the noise enough to confidently automate more decisions about whether to allow or deny transactions.

"Banks can accurately crack the case with an automated system that asks customers meaningful questions, as soon as a threat appears," says Rivner. "Customers will appreciate that their financial institution not only alerts them about possible scams but actively works with them to keep their money safe."

Methodology

This research was conducted online by Arizent in September 2025 among 114 banking professionals who have direct involvement with fraud analytics, operations, strategy, or policy at their organization.

About Refine Intelligence

Refine fights AI-powered fraud with customer-powered AI, that is, by teaming up with banks' best fraud fighters – their own customers. With fully automated digital inquiries, a rapid response rate and agentic AI capabilities, Refine enables fraud teams to catch more fraud and identity scams while dramatically reducing the daily workload of analysts, operations and frontline teams.

For more information, visit refineintelligence.com.

About Arizent Research

Arizent delivers actionable insights through full-service research solutions that tap into their first-party data, industry SMEs, and highly engaged communities across banking, payments, mortgage, insurance, municipal finance, accounting, HR/employee benefits and wealth management. They have leading brands in financial services including American Banker, The Bond Buyer, Financial Planning and National Mortgage News and in professional services, such as Accounting Today, Employee Benefit News, and Digital Insurance.

For more information, visit arizent.com.