Deception in the AI Age

Understanding, preventing & fighting financial scams

Thomson Reuters Institute

Executive summary

Victims' losses from financial scams reached approximately $20 billion in 2025, a 26% increase from the prior year.[1] Despite heightened regulatory attention and growing industry awareness, the scam landscape continues to accelerate in scale and sophistication.

Not surprisingly, AI has shifted scams from labor-intensive craft to comparatively easy algorithmic production. What once required call centers now runs on autonomous AI agents that test thousands of social engineering variants simultaneously, optimizing attacks in real time. Those professionals tasked with defending or fighting these scams face a fundamental constraint: Scams often involve willing victims who have passed security checks, leaving all the traditional fraud signals flashing green.

This is the Thomson Reuters Institute's first annual state of financial scams report, in which we hope to annually synthesize expert perspectives on the current state of scams, the transformative impact of AI on both criminal and defensive operations, and the operational challenges facing financial institutions, law enforcement, and consumers.

AI has shifted scams from labor-intensive craft to comparatively easy algorithmic production. What once required call centers now runs on autonomous AI agents that test thousands of social engineering variants simultaneously, optimizing attacks in real time.

Throughout our research, three findings illustrated how we understand scams and how that is changing:

First, scams are fundamentally different from fraud in ways that change how financial institutions detect them. Fraud is unauthorized activity, while scams involve victims who are *convinced to authorize* legitimate-looking transactions. Meaning the deception lies not in the transaction mechanics but in the victim's understanding of its purpose. This distinction explains why traditional transaction monitoring fails.

Second, scams are increasingly orchestrated from labor compounds in which human trafficking meets cybercrime. Criminal networks operate fortified facilities that use trafficked workers to execute fraud at industrial scale, creating a dual-victim model that compounds the human cost while driving the vast industrialization of the threat.

Third, current liability frameworks misalign incentives. Banks see the transaction but not the grooming. Social media sees relationship-building but not the financial harm. Telecoms see the social engineering but not the account takeover. No single actor has both visibility and control, yet liability concentrates in one place: the bank. This asymmetry must be restructured.

By looking into the changing state of financial scams, how they find and coerce victims, and how their illicit process is evolving with the use of advanced technology, financial institutions and fraud specialists can better prepare themselves for what is happening today and what is to come.

1 Federal Bureau of Investigation: *Internet Crime Report 2025*; *available at* https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf.

The state of scams: Today's threat landscape

While *fraud* and *scam* are often used interchangeably, they represent meaningfully different concepts with important implications for liability and legal analysis. Blake Howald, Senior Director of Data Science and R&D at Thomson Reuters Special Services (TRSS), says first, you have to look at how the bad actor is "trying to get something of *value* out of you" — it's about the value in the eye of the beholder.

Fraud involves unauthorized activity. An individual or organization takes action to obtain something of value from a victim without consent or knowledge. The hallmark of fraud is that the victim does not authorize the transaction.

Scams, by contrast, involve persuading the target to take an authorized action. The victim is convinced through deception, pressure, or false information to authorize a transaction. Although induced by misleading representations, the authorized action itself is technically legitimate. "A scam specifically involves social engineering," says Stephanie Macrafic, a certified fraud examiner at RiskScout. "And typically, the involvement and participation of the victim and deception that's convincing them to willingly participate in something that they don't really realize is fraudulent."

FIGURE 1:

Fraud v. scam: Why this matters

Fraud	Scam
Unauthorized activity	Authorized activity
Victim doesn't know a transaction occurred	Victim authorized the transaction
Bank sees the red flag (unauthorized access)	Bank sees a green flag (customer-initiated)
Detection: Look for the unauthorized act	Detection: Look for coercion intent
Example: Card skimming	Example: Tech support scam, romance scam
Liability: Rests on perpetrator and institution security	Liability: Complex & victim authorized it

Source: Thomson Reuters 2026

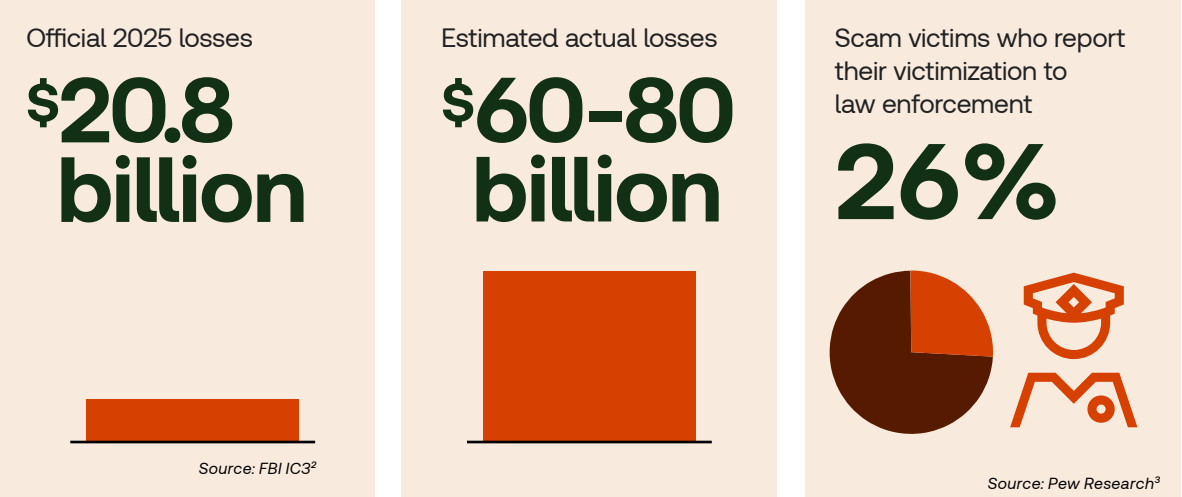
This distinction is not merely academic; it shapes how financial institutions detect, investigate, and respond to illicit transactions. "In many ways, the bank sees an authorized payment, the customer believes they are making the right payment, and only the criminal knows the truth," explains Mikhail Karataev, an anti-money-laundering analyst with Citi. "That is why money laundering disguises where money came from; and scams disguise why the money is being sent." Karataev's framing underscores why authorized-transaction scams pose a unique detection challenge for banks, because unlike fraud, in which an unauthorized transaction itself can serve as a red flag, scams present as legitimate, customer-initiated activity. And that means the deception lies not in the mechanics of the payment but in the victim's understanding of its purpose.

Further, this authorization element creates meaningful differences in liability assessment. In fraud cases, liability questions focus on the perpetrator's conduct and whether adequate safeguards prevented unauthorized access. In scam cases, analyses become more complex because the victim has authorized the activity.

FIGURE 2:

The reporting gap: The core problem

Official reported losses are catastrophically incomplete.



Source: Thomson Reuters 2026

This gap in estimated losses and victim reporting is systematic. Victims don't report because of shame, embarrassment, distrust, or belief that nothing will happen. However, this creates a blind spot because institutions believe the problem is three or four-times smaller than it is, so they under-invest in prevention.

If the 1 million complaints to the FBI's Internet Crime Complaint Center (IC3) represent only 26% of actual scams, the true annual incident count in the United States is roughly 3.8 million with most being invisible to law enforcement and institutional risk models.

AI is changing the game

In 2025, complaints referencing AI accounted for just 2.2% of all complaints — but 4.3% of total financial losses. The average loss per AI-related incident was nearly twice that of other incidents: $39,935 compared with $24,100.[4]

One reason this might be is that AI scams are more convincing (fewer victims recognize and report them), target higher money amounts (criminals use AI for more sophisticated attacks), and carry disproportionate shame (victims don't report because they believe they should have detected the deepfake). The result of this is that AI scams are growing faster than non-AI scams.

As the above graphic shows, the institutional picture is stark. Financial institutions proactively detect only 10% to 15% of annual losses and recover just 2% to 5% of the amounts identified, largely because real-time payments leave little opportunity to retrieve funds. Institutions are therefore confronting a problem many times larger than their data suggests while recovering almost nothing after the fact, making *prevention* the only viable strategy.

2 Federal Bureau of Investigation: *Internet Crime Report 2025*; *available at* https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf.

3 Pew Research Center: July 31, 2025; *available at* https://www.pewresearch.org/internet/2025/07/31/online-scams-and-attacks-in-america-today

4 Federal Bureau of Investigation Press Release April 6, 2026; *available at* https://www.fbi.gov/news/press-releases/cryptocurrency-and-ai-scams-bilk-americans-of-billions

Uri Rivner, CEO and co-founder of Refine Intelligence, says the situation resembles "freak weather" that's unpredictable in its specifics but certain in its trajectory. "We don't know exactly what's coming," Rivner adds. "But it will get worse, not just in terms of the scale of those attacks, but in terms of the fact that it's no longer going to be, 2026 versus 2025. It's going to be this week versus last week. It's going to be today versus yesterday. The pace of change will be dramatic."

This acceleration has given rise to what industry *observers now call the scampocalypse*,[5] a massive global rise in sophisticated social engineering and authorized push-payment fraud. "The scampocalypse will absolutely continue," says Julie Conroy, a board member of The Knoble, a global network of financial crime professionals. "It's so hard to determine intent when you're trying to interact with a consumer." The difficulty of distinguishing legitimate transactions from fraudulent ones in real time lies at the heart of why this problem persists and is growing.

Complicating matters further, older fraud schemes such as check scams — in which oversized checks are received with instructions that to deposit it and wire back a portion, then the check later bounces, leaving the victim liable — continue to thrive alongside new threats like deepfakes and synthetic identity theft. Check scams continue because they still work. Deceptive email phishing still works. Romance scams — in which fraudsters build fake romantic relationships over weeks or months, then request money — still work.

Yet now each can be enhanced: A check scam can be paired with AI-generated verification documents; a phishing email can be personalized using social-media-scraped data and voice-cloned from a deepfake recording. "This convergence isn't replacement, it's weaponization," Conroy explains. "Criminals don't abandon working methods; they layer new tools onto them. This means institutions defending against 2024 tactics are simultaneously blind to 2026 variants."

These forces, human susceptibility, technological acceleration, and the layering of old and new methods, are all combining to form what some experts describe as a *scam economy*.

FIGURE 3:

The acceleration timeline

2024-2025:
Week-to-week evolution

- New scam variants introduced weekly
- Institutions patch; criminals adapt
- Lag time: Days to weeks

2026 (Current):
Day-to-day sophistication

- Scammers test new social engineering daily
- AI agentic systems run concurrent variants
- Lag time: Hours

2027 Trajectory:
Hour-to-hour autonomous adaptation

- If agentic AI deploys at scale without human operators, attacks become:
  - Continuous (24/7, not business hours)
  - Adaptive (responding to defense changes in real time)
  - Personalized (unique approach for each victim based on behavioral profile)
  - Distributed (no geographic concentration to monitor)
- Lag time: Minutes

What this means for defense: Reactive detection fails entirely, and prevention becomes mandatory.

Source: Thomson Reuters 2026

5 *Scams: On the Precipice of the Scampocalypse*: March 9, 2022; *available at* https://datos-insights.com/reports/scams-precipice-scampocalypse/

Scam economics and criminal infrastructure

Today, even the places where scams happen have changed dramatically. So-called scam compounds are large, fortified facilities operated by organized criminal networks in which hundreds of individuals are confined and compelled to execute online financial fraud on an industrial scale.

"This is not like a lone wolf in their mom's basement," observes Stacey Wishowsky, a Senior Solutions Consultant for ID verification platform Socure. "These are organized rings, and the money often goes to things that are not just someone living a lavish lifestyle... it's funding things that are pretty scary in the world."

These operations integrate human trafficking with global cybercrime in a dual-victim model, exploiting both coerced workers and defrauded targets simultaneously.

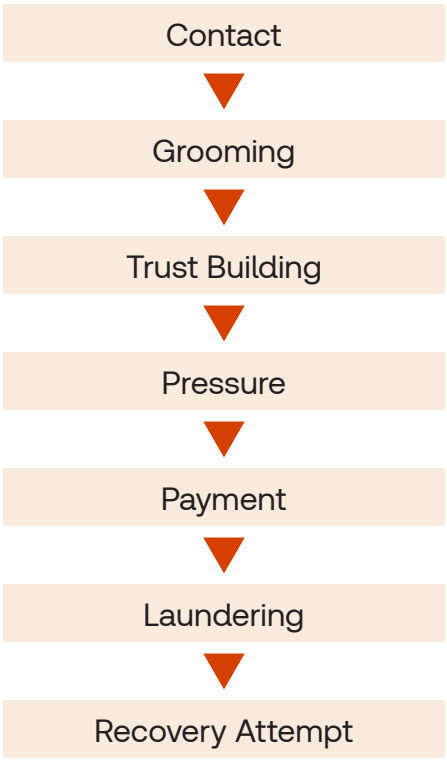
The scale of scam compound operations remains undercounted. Law enforcement has documented compounds in Southeast Asia and West Africa, but systematic data collection is minimal. This gap in data understanding itself is evidence of the problem's institutional invisibility.

Worse yet, human trafficking serves as the labor engine. By controlling workers through coercion, debt bondage, or physical confinement, criminal organizations achieve minimal overhead: no wages, restricted food costs, and eliminated living expenses. This transforms scams from distributed activity into centralized production, aggregating thousands of small-scale deceptions into substantial revenue streams.

Trace Fooshee, Strategic Advisor at financial service research firm Datos Insights, notes how this mass expansion of scams makes it harder for individual financial institutions to catch. "A scam is a mile-long journey, and the financial institution only sees the last few feet of it" Fooshee says. "The bulk of that mile-long journey happens on a variety of different social platforms." Indeed, victim contact and grooming may occur on social media while financial institutions intercept only the final transaction layer.

FIGURE 4:

Scam-lifecycle framework



Actor	What they see
Social media	Contact/Grooming
Telecom	Communication
Bank	Payment
Law enforcement	Aftermath

Source: Thomson Reuters 2026

Further, money mule networks — in which victims are recruited for money forwarding roles that facilitate money laundering — function as financial logistics, comprising individuals, shell companies, and bank accounts that layer illicit proceeds through multiple transfers. They obfuscate audit trails, enable jurisdictional arbitrage across regulatory gaps, and manage volumes that would trigger alerts if centralized.

These operations are within broader organized crime ecosystems providing capital, logistics, cross-border coordination, and enforcement capabilities. This integration explains their resilience against law enforcement pressure.

Industrialization stems from structural factors: digital scalability allowing one operation to target millions; trafficked workers providing flexible, low-cost human capital for social engineering; asymmetric risk distribution that insulates operators; regulatory lag outpacing cross-border coordination; and accessible technology lowering entry barriers.

The result is an inherently transnational enterprise with infrastructure in low-enforcement jurisdictions, targets across wealthy nations, financial flows through multiple regimes, and leadership beyond easy extradition. No single agency possesses the mandate to dismantle the entire ecosystem. Interventions targeting only one element are absorbed by the system's inherent flexibility.

Labor compounds: The supply-side transformation

Scam compounds are not incidental to the industry; indeed, they are its economic foundation. Organized crime groups deliberately employ trafficked workers because the business model is irresistible.

Consider the overhead. A traditional call center operating with 100 workers costs approximately $600,000 annually in salaries alone. A scam compound housing the same number costs roughly $60,000: no wages, minimal food costs, controlled confinement. The margin difference of $540,000 per compound per year is reinvested into recruitment, technology, and enforcement. This explains why industrialization is accelerating faster than law enforcement can respond.

What makes the ecosystem self-perpetuating is the victim pipeline. Many workers confined in compounds are prior scam victims, initially recruited as money mules, then trapped through debt bondage or threats. This creates a closed loop: victims become mules; then mules become workers; and finally, workers generate new victims whose funds flow through the same networks.

In this structure, trafficked workers handle the most labor-intensive phase, building relationships, establishing trust, grooming victims over the course of weeks. Once emotional investment peaks, handoff occurs to AI systems for final pressure and payment extraction. By 2027, as agentic AI eliminates the need for human operators, this model may become obsolete. Until then, scam compounds remain the leverage point at which enforcement can disrupt the entire chain.

Agentic AI & the new scam economy

AI hasn't just improved scamming, it has industrialized it. AI lets criminals test pretexts against real victims in real time, clone voices, write convincing phishing copy, and mimic institutional tone with minimal skill. Autonomous agents now run thousands of simultaneous scams at near-zero marginal cost, turning a once labor-intensive crime into an industrial one.

The technology itself, however, is agnostic. "It's not just necessarily that AI is bad," explains Matt Killam, Senior Investigator for GEICO. "It's more of the aspect that people can use it. It's the end user of the AI that is bad." Indeed, the same efficiencies boosting legitimate businesses also are boosting fraud, at a scale most defenses were never built to handle.

And now, a second inflection point is imminent. Agentic AI will eliminate the need for human operators entirely, possibly the thousands victimized by scam compounds worldwide. Organized crime groups will instead deploy autonomous systems that handle entire victim journeys end-to-end. This will test varying approaches continuously, adapting to defenses in real time, and operating 24/7 without fatigue or error.

The operational consequence is stark, even if scam compounds become obsolete. If you can automate contact entirely, confinement becomes unnecessary and criminal infrastructure will shift to distributed servers nearly anywhere. Profit margins will improve, and detection risk will decline as sophistication accelerates.

For financial institutions, this means defenses that are optimized for human-operated scams become obsolete as well. Behavioral biometrics that catch hesitation mean nothing if no human hesitates. Instead, prevention will become mandatory.

This inflection point is imminent, but not inevitable. Financial institutions have about 12 months to prepare.

AI as a weapon

AI has eliminated the traditional barriers to sophisticated scamming, and agentic AI is only going to take things further. "AI can be used today to test out new social engineering methods," says Refine Intelligence's Rivner. "You can basically let AI loose on victims and tell the AI just try stuff (such as scams or plots) and tell you what's working." Rather than manual trial-and-error, scammers can now run thousands of experiments simultaneously to optimize their attacks.

And technical expertise is no longer required. "You do not have to be sophisticated, smart or a technical wizard — you can be an average Joe," observes Lesley Park, Global Director of Financial Services at Thomson Reuters. "And with the help of AI, you can run a sophisticated scam. That's terrifying."

Garrett Sadler, Senior Account Executive at financial crime-fighting platform ThreatMark, agrees, warning that the biggest shift over the next few years will be scams increasingly using AI, and specifically agentic AI. "No longer will organized crime groups need to have a call center of 100 people," Sadler explains. "As organized fraud groups start leveraging more agentic AI, I think we'll see more smarter scams, faster scams, and at more volume."

Deepfakes, voice cloning, synthetic identities, and grammatically perfect phishing will then eliminate the traditional tells that once exposed scams. “Now, you don’t need a Masters in large language models in order to build tools,” notes Ayelet Biger-Levin founder of RangersAI, a platform that helps financial institutions empower their customers to recognize and prevent scam communications early. “So that’s a big change for the criminal economy.”

AI as defense

Using AI, attackers can innovate faster than defenders can deploy. By the time a bank detects a new scam variant and implements a response, scammers have already moved to the next variant. This isn’t a technology gap, it’s a structural gap.

For banks’ financial crime prevention teams to shift from *detecting known scams to predicting unknown scams* requires behavioral intent analysis (not just transaction monitoring) and real-time intervention (not just post-incident forensics). Both are technically possible but currently, operationally rare.

For financial institutions not to be swept away by the agentic AI onslaught, that is going to have to change — and quickly.

Where do financial institutions go next?

Given the rapid advancement of advanced AI technology and what that enables, financial institutions’ main strategy should be a sharp shift toward prevention. “In order to effectively fight scams, we need to put controls across the scam life cycle, but we really need to start with preventing the scam,” argues RangersAI’s Biger-Levin. “Scam prevention is a new customer success — it’s really helping guide your customer. The banks are on the front lines for these activities, and so it’s expected of the banks to go above and beyond to protect their customers.”

This strategic refocus can reposition prevention not as compliance burden but as customer success imperative. Because financial institutions intercept the transaction’s final stage, they possess both the visibility and the obligation to intervene before funds leave the system… and the customer’s account.

Preventing scams

Effective prevention operates through a layered defense model that includes consumer education, institutional controls, and network-level signals that all work in concert.

At the individual level, for example, the priority for investigators or fraud specialists is interrupting impulses. Howald of TRSS notes that the number one defense really is just taking a breath. “If you wait even 5 minutes, 10 minutes, get up from your desk, go for a walk,” he suggests. “Just allow yourself to reset and look at it with fresh eyes.” This simple pause can prevent losses of tens of thousands of dollars.

FIGURE 5:

Interrupting scams

Individuals should watch for *PAUSE* triggers:

P	**Pressure** Pushed to act immediately, no time to think
A	**Advance payment** Asked to pay before receiving anything
U	**Urgency** Threats of a deadline, loss or penalty
S	**Strange requests** Unusual payment methods or instructions
E	**Excessive contact** Repeated calls or messages to keep control

At the institutional level, financial services firms should *WAIT*:

W	**Withhold transaction** Hold before the transaction completes
A	**Ask questions** Question the customer about the request
I	**Investigate** Review account history and red flags
T	**Train employees** Reinforce fraud awareness training

Source: Thomson Reuters 2026

The Knoble's Conroy notes that this approach is already reshaping industry norms. "As you have any sort of thought that this might be a scam, delay," she says. "Real-time payments in Australia are no longer real-time payments because they delay. Anytime they think it might be a scam, they put a three- to nine-hour hold on it to give the person the time to kind of have the buyer's remorse. I think right now, that's their best option." The challenge for institutions, however, is to maintain the speed customers expect while introducing enough friction to stop suspicious payments before harm occurs.

Further, AI and technology can support earlier intervention through the use of behavioral biometrics at account opening, real-time transaction scoring, natural-language tools that identify scam scripts in calls and chats, and predictive models that flag at-risk customers before funds are transferred.

"If you are able to train the AI to recognize customer intent, that would give the AI an edge to do the investigation automatically," explains Refine Intelligence's Rivner.

The balance between a positive customer experience and enough friction to prevent scam losses is a central tension for financial institutions. The solution is designing prevention methods that protect without alienating legitimate customers. This means positioning trust as a competitive advantage, not merely a security measure.

For example, data sharing between platforms can close the information gap. Banks see the money moving, and meta platforms see the grooming and early contact. Yet, neither has the complete picture alone. When banks work together through shared fraud databases, coordinated account freezes, and joint work with law enforcement, they can amplify fraud-fighting efforts against money mule networks and large scam operations.

This prevention approach achieves what enforcement alone cannot: It stops scams before money enters the financial system, reduces harm to customers, and shifts risk back toward criminal operators rather than their victims.

The detection paradox

A bank's fraud detection system is trained on one principle, to spot unauthorized transactions.

However, in many scams, victims authorize the transaction, often initiating it themselves. The victim passed security checks, authenticates their actions, and all fraud signals are green.

Traditional transaction monitoring fails when scams involve authorized payments by coerced victims. That's why banks' detection must shift from verifying identity to analyzing intent through behavioral analytics. Session data, hesitation, and active phone calls during banking sessions provide the context that raw transaction data lacks.

If needed, direct customer outreach should also be used to discover intent — and AI can now analyze the customer explanation as well. "Not talking to the customer is a little bit like a detective who doesn't talk to the key witness," Rivner adds.

FIGURE 6:

Key indicators of coercion

Indicator	Legitimate signal	Coercion signal	Risk level
Session duration	Normal banking session	Rapid escalation (2-3 min. to large transfer)	Medium
Transfer size	Gradual increase over time	First transfer is unusually large	High
Destination type	Repeating payee, known recipient	New payee, atypical destination	High
Customer affect	Calm, deliberate	Rushed, anxious, hesitant	Medium
Inquiry pattern	No questions, routine	Unusual verification questions	High
Timing	Typical banking hours	Off-hours or weekends	Medium
Device change	Consistent device	New device used for large transfer	Medium
Call during transaction	Customer call bank proactively	Customer is on phone with third party during transfer	Very high

Source: Thomson Reuters 2026

AI-driven detection models are essential at scale, but they need richer context to separate coerced transactions from legitimate ones. Because real-time payments leave little chance for recovery, institutions must intervene before funds exit the account.

ThreatMark's Sadler emphasizes the shift required: "The way to do that is not to be really good at saying, *Hey, a scam happened*, but being really good at saying, *Hey, a scam is going to happen*." That calls for real-time intervention strategies, Sadler adds, including targeted friction, payment delays, and interactive questioning — all of which should be guided by early warning signals rather than after-the-fact forensics.

In addition, no single institution sees the full picture, making network analytics and consortium data essential. “Everything that happens beyond your four walls is just as important as what you’re seeing within your own four walls,” says Park, of Thomson Reuters. Effective detection requires shared intelligence across banks, payment networks, telecoms, and social platforms, she notes.

Fortunately, the technology to help with all this exists; however, the gap lies in implementation, data sharing, and the willingness to introduce friction into a no-friction-obsessed industry.

Using AI to investigate scams

AI use by the financial services industry for scam prevention is a necessary countermeasure to AI-enabled scams, but it only works when paired with the right context. AI tools can detect deepfakes, synthetic documents, and AI-written scam scripts while helping investigators triage cases and link related incidents at scale.

However, effective automation requires more than using the same data that was used for detection. Enriched signals, especially indicators of customer intent, are what turn raw alerts into actionable intelligence for law enforcement referrals.

Effective automation requires more than using the same data that was used for detection.

Unfortunately for many financial institutions, operational readiness remains the bottleneck. Fraud teams face staffing shortages, uneven training on emerging scam typologies, and tools that leave analysts manually connecting data across siloed systems. Early-layer mitigation tactics — such as phishing infrastructure detection — can prevent many scams before investigators are forced to chase funds through layered accounts, cryptocurrency, or offshore mule networks.

Yet, without enterprise-level data sharing and standardized investigation protocols, the gap between scam sophistication and investigative capacity will continue to widen.

Closing the liability gap

Finally, work needs to be done to close the liability gap that often leaves victims bearing losses while scammers operate with impunity. The consensus is shifting toward shared responsibility among institutions that actively participate in payment flows. The United Kingdom has led this trend by establishing that banks benefiting from these flows must invest in their security.

Under the UK model, liability is split 50/50 between sending and receiving institutions. This incentivizes receiving banks to scrutinize accounts serving as mule hubs — and this kind of operational accountability is a good thing, says Urriolagoitia (Rio) Miner, CEO of FCI Tradecraft. “Banks have a know-your-client requirement, and they onboarded a scammer,” he says. “It’s very interesting that they’re allowed to onboard whomever and make money off of owning that account.”

However, the most effective approach allocates liability based on control and visibility. “Organizations should be held accountable in proportion to their ability to prevent or detect harm,” explains Melissa Coutier, Founder of the Compliance Shop and an Association of Certified Fraud Examiners (ACFE) leader. “A high lack of controls or internal control breakdown would hold you more liable.” When institutions profit from transaction flows, accountability must follow, she adds.

Indeed, limiting liability to banks overlooks the full scam lifecycle. As mentioned earlier, financial institutions often see only the final step in a much longer scam journey that begins with social engineering on social media and telecommunications platforms. Responsibility should follow both harm and control. Where organizations can detect anomalies or disrupt abuse, they should be expected to act.

Effective scam prevention requires a shared responsibility model that maps accountability across the entire ecosystem. “Safety and security are in everyone’s interest,” says Datos Insights’ Fooshee. “It’s going to take a degree of collaboration and partnership across the whole of the ecosystem. This is not something that we can simply pin on banks or something that we can simply shunt to the government.”

By distributing liability according to where harm occurs and where control exists, the ecosystem can move from a reactive posture to one of collective defense. As Park explains, until every actor has skin in the game — from the social platform enabling the first contact to the bank processing the final wire — the incentives to prioritize security over speed or profit will remain misaligned.

What’s on the horizon?

The next 12 months will determine institutional readiness for the immediate future. This is not hyperbole — if agentic AI adoption accelerates as expected, criminal organizations may increasingly replace human operators with autonomous systems by next year.

Financial institutions that wait to deploy behavioral analytics will find their defenses obsolete; and those that rely on law enforcement data to size the threat will remain blind to the actual scale of victimization, which may be as much as four-times what is reported. And institutions that have not joined a consortium that better allows for mule detection will lack the visibility necessary to prevent organized money extraction. In short, institutions have 12 short months to move from their current reactive posture to proactive defense.

In short, institutions have 12 short months to move from their current reactive posture to proactive defense.

The responses will differ by institution type, of course. Large banks with substantial capital likely will adopt 50/50 liability models internally, deploy behavioral analytics across real-time payment channels, and establish dedicated scam investigation units separate from their fraud teams. These larger institutions will differentiate themselves through visible scam prevention, which is becoming a competitive advantage in a market increasingly skeptical of trust in digital commerce. Regional banks, on the other hand, may lack the infrastructure to compete and will choose to outsource detection to third-party vendors, accepting higher loss rates as the cost of their scale limitation.

Meanwhile, fintech and emerging platforms will be most aggressive on innovation around prevention but will face regulatory scrutiny and reputation risk. Payment networks will shift from optional to mandatory consortium participation; and social platforms will face regulatory pressure and will improve detection voluntarily to protect their brand, even while resisting overall liability.

Law enforcement, for its part, will move past individual scammer prosecution in favor of disrupting organized crime infrastructure and working with international task forces to focus on scam compounds.

The competitive outcome is clear: Those institutions deploying behavioral analytics and joining consortium-provided mule detection by mid-2027 will own the landscape. Those that wait will face regulatory backlash, market share loss, and catastrophic exposure when fully autonomous scams swing into action.

Taking action

For the most part, scams have not changed — they still rely on deception, urgency, and manufactured trust. What has changed is their scale, speed, and fundamental nature.

Within 12 months, agentic AI will shift scam operations from labor-intensive to autonomous. After that point, the scams that devastate institutions will be virtually undetectable using current approaches. AI has made scams more persuasive and personalized, while real-time payments have compressed the window for intervention. The response from financial institutions must move upstream, before victims authorize payments and before funds become difficult to recover.

Immediate action starts with simple friction. As mentioned above, the PAUSE and WAIT frameworks create spaces to stop, verify, and involve others before acting for consumers and financial institutions alike. Indeed, WAIT offers an operational response that urges institutions to withhold suspicious transactions, ask targeted questions, investigate patterns, and train staff to recognize scam indicators *without* blaming the customer.

Longer-term progress requires shared defenses that no single actor can build alone. Banks, payment networks, telecoms, social platforms, regulators, and technology providers each see a part of the victim's scam journey. Coordinated data sharing, stronger mule-account detection, AI-assisted investigations, liability frameworks that reflect control and harm, and real-time behavioral monitoring are all necessary tools to close the gaps that criminals exploit.

The bottom line is that scams scale toward weakness. Any durable response will depend on making the ecosystem harder to exploit, aligning incentives across sectors, and introducing targeted friction in those instances in which it can prevent irreversible harm.

The future of scam prevention is not detecting bad transactions, rather it's recognizing bad intent before a good customer tries to authorize one.

Appendix

Methodology

This report draws upon insights from 13 interviews conducted in July and August 2026 with subject matter experts across the United States. The interview cohort included fraud investigators, behavioral biometric specialists, financial crime analysts, former federal agents, strategic advisors, and technology founders, each selected for their relevant expertise regarding AI, financial crimes, frauds, and scams.

Interviewees represented a range of technical proficiency levels and brought diverse professional perspectives to the discussion. All participants contributed in their personal capacity, and their views do not represent the official positions of their respective organizations or employers.

Interviewees

1. **Ayelet Biger-Levin**
   RangersAI – https://www.rangersai.com/about
2. **Julie Conroy**, Board Member
   The Knoble – https://theknoble.com
3. **Melissa Coutier**, Founder,
   Compliance Shop – https://www.businesscomplianceconsulting.com
   Association of Certified Fraud Examiners (ACFE) Leader – https://www.acfe.com
4. **Trace Fooshee**, Strategic Advisor
   Datos Insights – https://datos-insights.com/about-us
5. **Blake Howald**, Senior Director, Data Science and R&D
   Thomson Reuters Special Services (TRSS) – https://www.trssllc.com
6. **Mikhail Karataev**, Anti-Money Laundering Analyst
   Citi – https://www.citi.com
7. **Matt Killam**, CFE, MBA, OSC Senior SIU Investigator
   GEICO – https://www.geico.com
8. **Urriolagoitia (Rio) Miner**, CEO
   FCI Tradecraft – https://fcitradecraft.com
9. **Lesley Park**, Global Director, Financial Services Industry Lead
   Thomson Reuters – https://www.thomsonreuters.com
10. **Stephanie Macrafic**, CFE
    RiskScout/ACFE – https://www.riskscout.com
11. **Uri Rivner**, CEO and co-founder
    Refine Intelligence – https://www.refineintelligence.com
12. **Garrett Sadler**, Senior Account Executive
    ThreatMark – https://www.threatmark.com
13. **Stacey Wishowsky**, Sr. Solutions Consultant
    Socure – https://www.socure.com

Thomson Reuters

Thomson Reuters (*TSX/Nasdaq:* TRI) informs the way forward by bringing together the trusted content and technology that people and organizations need to make the right decisions. The company serves professionals across legal, tax, audit, accounting, compliance, government, and media. Its products combine highly specialized software and insights to empower professionals with the data, intelligence, and solutions needed to make informed decisions, and to help institutions in their pursuit of justice, truth, and transparency. Reuters, part of Thomson Reuters, is a world-leading provider of trusted journalism and news.

For more information on Thomson Reuters, visit **tr.com** and for the latest world news, **reuters.com**.

Thomson Reuters Institute

The Thomson Reuters Institute brings together people from across the legal, corporate, tax & accounting and government communities to ignite conversation and debate, make sense of the latest events and trends and provide essential guidance on the opportunities and challenges facing their world today. As the dedicated thought leadership arm of Thomson Reuters, our content spans articles and commentaries, industry-leading reports and data sets, informed analyses, interviews with industry leaders, videos, podcasts, and world-class events that deliver keen insight into a dynamic business landscape.

Visit **thomsonreuters.com/institute** for more details.

Thomson Reuters Institute