WHITEPAPER

Fraud & AML Trends in Financial Services

sardine

Table of contents

Foreword

Looking back at my 2024 predictions, several materialized faster than anticipated. Generative AI has transformed from a buzzword into a tangible threat, with 42% of scams now being AI-driven. First-party fraud has evolved from a growing concern into a primary challenge, while deepfake attacks during onboarding have shifted from theoretical risk to operational reality.

The financial crime landscape has fundamentally shifted. The volume, sophistication, and speed of attacks have outpaced traditional approaches. But the same technology driving these threats is now helping risk teams transform their operations and build better defenses. At Sardine, we've proven our AI-powered models can see through the user's device and behavior to catch early warning signals of deepfakes and bots before they cause harm.

The future belongs to risk teams that combine massive data sets, cross-industry intelligence, lightning-fast decisioning capabilities, and AI agents that augment the humans in the loop. We're already seeing clients "go full platform" as they recognize the compound advantage of this integrated approach.

Last year, a tier 1 bank discovered that Sonar could have prevented nearly 42% of wire fraud by predicting which wires were being sent to a crypto exchange for a social engineering scam. This success underscores a broader shift: we now have the tools to not only anticipate attacks but also prevent them in real-time.

This is the turning point. 2025 is the year we fight back.

At Sardine, our mission remains constant: to solve financial crime and unlock commerce. In 2025, we'll continue to lead this evolution, delivering the data, AI, and tools needed to stay ahead of increasingly sophisticated threats. The challenge is enormous, but so is the opportunity. Together, we can build a financial system that's both more accessible and more secure.

If you're ready to prepare for the challenges ahead, let's discuss how Sardine can help solve your specific needs for 2025 and beyond.

Let's dive in.

Soups Ranjan
Co-founder, CEO
Sardine

Trend 1

Scams Become the Defining Challenge in Finance

In 2024, we predicted a regulatory clampdown on scams as losses continued to mount. That prediction proved accurate, but as is often the case in financial services, the response has introduced its own new challenges. While major banks began refunding Authorized Push Payment (APP) scam victims - a laudable step - we've seen an uptick in first-party fraud, where bad actors attempt to exploit chargeback and reimbursement systems under the guise of legitimate claims.

The problem? Reimbursing victims treats the symptom, not the disease. This was my core message when I spoke at the UK's house of lords, and it's something we see in the data today.

In 2025, we'll see this challenge reach critical mass:

- AI-generated scam content will become increasingly sophisticated.
- Social engineering attacks will leverage deepfake technology for voice and video.
- Scams that start in social media, then move to crypto and banking exploit the gaps between companies, networks and industries.
- First-party fraud will continue its explosive growth.

The intersection of these trends creates a perfect storm. Financial institutions can't simply write off these losses - the numbers are too large. They can't just add friction - the competition is too fierce. They need a new approach entirely.

> "**AI-assisted fraud and deepfakes** continue to be on the rise. We're going to see a lot more fraudsters using AI to create highly realistic images, video, and audio that imitate individuals, leading to an uptick in identity theft, account takeovers, and other scams."

Sarah Mirsky-Terranova
Owner and Principal, AE Consulting

What we see our strongest customers doing is doubling down on ML/AI and training custom models to pick up on unique risk flags. They're also participating in cross-industry consortiums to close up key data gaps. And they're making heavy investments into AI to beef up their risk operations.

Nayeem Mano, VP of Risk & AML Compliance at Paylocity, echoes this shift:

> “With global payment fraud losses projected to surpass $48 billion, the industry must shift from reactive compliance to predictive intelligence. At Paylocity, partnering with Sardine has empowered us to stay ahead leveraging real-time monitoring and AI-powered insights to safeguard not just transactions, but trust itself.”

Nayeem Mano
Airbase VP of Risk & AML Compliance, Paylocity

Trend 2

AI Agents Transform Risk Operations

The rise of AI agents is perhaps the most transformative trend in fraud and compliance today. As alerts and SAR filings continue to skyrocket with no sign of stopping – up 800% in just the past few years – risk leaders have come to terms with the fact that you can’t hire your way out of an 8X increase in monthly alerts.

↑ 800%

Skyrocket in **alerts and SAR filings**

Instead, we’re seeing an increased adoption in AI agents and copilots to help their teams handle the load. These aren’t just enhanced automation tools – they’re intelligent systems that manage routine tasks, process massive datasets in seconds, and escalate complex cases when human judgment is required.

Today, Sardine customers are using AI agents to:

- Review sanctions alerts
- Manage dispute resolution
- Review customer onboarding documents
- Pre-screen transaction monitoring alerts
- Assist in SAR narrative creation and evidence collection
- Conduct initial investigations to save time
- Improve capture rates through improved pattern recognition

For instance, we've been using our dispute resolution agent as a support for our payments team. We equipped it with templates for all the major processors and our team's playbook for winning disputes, and now the agent speeds up our process significantly. It selects the right template based on processor and dispute type, assembles evidence including device data for Compelling Evidence 3.0 when required, and submits it directly to card schemes like Visa and MasterCard once our Payment Ops Manager gives it the thumbs up.

> "Our disputes agent has been a game-changer for our payments team. Equipped with our templates and playbooks, it's driving a 7x increase in efficiency. What used to take 35 minutes per form now takes just 5 minutes."
>
> 
>
> **Soups Ranjan**
> CEO and Founder, Sardine

Jas Randhawa at StrategyBrix also notes that AI Audits are a huge area of opportunity: "AI-driven systems will be capable of analyzing vast amounts of documents and transaction data, identifying complex patterns, and detecting anomalies with remarkable precision. LLMs will excel at processing and interpreting unstructured text, enabling auditors to quickly sift through regulatory documents, internal policies, and customer communications."

This is what's making the potential of AI copilots so exciting for risk leaders, and we expect to see a lot more of it in 2025.

Trend 3

Cross-Sector Data Sharing Reaches Critical Mass

This past year, we saw countless LinkedIn posts with screenshots from Telegram groups and other forums where fraudsters are actively collaborating. The message was clear: if fraudsters don't operate in silos, neither can we.

While cross-industry data sharing has already proven its value within specific sectors, this year the risk industry really stepped it up. Our Sonar consortium saw unprecedented growth as traditional players partnered with startups to plug critical data gaps. For instance, one tier 1 bank discovered that Sonar could have prevented nearly 42% of wire fraud by identifying wires being sent to crypto exchanges as part of social engineering scams.

42%

Of wire fraud could have been prevented by Sonar

This past year, we saw countless LinkedIn posts with screenshots from Telegram groups and other forums where fraudsters are actively collaborating. The message was clear: if fraudsters don't operate in silos, neither can we.

In 2025, we expect data sharing to expand dramatically:

- Cross-industry consortiums that allow for data sharing across financial services as well as telcos & social media companies will form to combat common threats.
- Real-time threat intelligence sharing will become standard.
- Regulatory frameworks will evolve to encourage responsible data sharing.
- Privacy-preserving technologies will enable broader collaboration.

The math is simple: more data means better models. Better models mean fewer losses. The organizations participating in these networks will have a significant advantage over those not.

Trend 4

Fraud Model Validation Becomes a Regulatory Focus

Another emerging trend that deserves every compliance leader's attention is the increasing regulatory scrutiny around fraud model validation. Recent years have seen several high-profile banks, fintechs, and crypto exchanges falter, leaving customers in the lurch and forcing regulators to step in. The question regulators are now asking is simple: are your risk controls effective and working as intended?

The challenge, however, is that "model validation" means different things to different people, making it a moving target for financial institutions and fintechs.

Our general counsel, Christine Poulon, notes:

> "While regulators have long required rigorous validation for compliance models, we expect fraud models will face increasing regulatory scrutiny in 2025. This shift will be particularly relevant for fraud prevention systems that overlap with compliance functions, such as KYC and identity verification."

Christine Poulon
Head of Legal & Compliance, Sardine

Regulators are asking pointed questions in three key areas:

- **System effectiveness:** Are your models doing what they're supposed to do, and are the results measurable?
- **Custom configuration:** Are your systems tailored to your use case, or are you relying on "out-of-the-box" rules from providers that may not align with your risk profile?
- **Model transparency:** Can you explain how your machine learning models work, and are they combatting the "black box" reputation some ML/AI systems often carry?

In 2025, expect:

- Stricter requirements for model explainability
- Regular validation of ML and AI system effectiveness, with an emphasis on stress testing and risk assessments
- Greater scrutiny of "out-of-the-box" solutions, requiring firms to demonstrate how they tailor vendor models to their specific risk environments
- Mandatory documentation of model decision-making
- Increased validation requirements on traditional rule-based engines

As someone who has been deep in machine learning for over a decade, I know that ensuring our systems work as intended – and can be **measured, explained, and improved** – is critical as they become more autonomous. **Explainable models are models we can evaluate. And if you can evaluate it, you can improve it.** This will be a major focus for us in 2025.

One counterintuitive insight from Jas Randhawa is that this regulatory focus could create an ideal environment for robotic process automation (RPA). While AI and LLMs are advancing rapidly, he believes their **black box** nature and **unexplainable decisions** could slow widespread adoption in AML compliance. Instead, regulators may favor **RPA's rule-based approach** for automating routine compliance tasks, as it aligns more closely with regulatory expectations.

> "RPA's rule-based approach and ability to automate routine tasks, aligns more closely with regulatory requirements and offers a pragmatic solution. By 2025, RPA models could dramatically reduce average alert handling times, potentially cutting basic AML check durations by up to 70-75%."

Jas Randhawa
CEO and Managing Partner, StrategyBRIX

Trend 5

Tech-enabled Fraud & Compliance integration cuts investigation manual effort and fraud rates.

Fraud and compliance teams continue to become more connected than ever, and for good reason. Systems that can link possible first-party fraud, like mule activity, to ongoing investigations or criminal networks in real-time not only prevents fraud, but also ensure a complete audit trail is maintained for compliance purposes.

Critics were vocal in 2024 about why FrAML – combining fraud and compliance – will never work, insisting these teams and functions should remain separate. But regardless of where you stand on that debate, one fact is clear: the value of collaboration and data sharing between fraud and compliance is undeniable (and should be non-negotiable).

Sharing risk signals and tools like ML models, network graphs, and even rules engines doesn't just cut costs by eliminating duplicate spending, it also closes critical data gaps that fraudsters are quick to exploit.

In 2025, we'll see:

- Models that learn from both fraud and compliance signals in real-time (not just shared data, but shared intelligence).
- Platforms that handle the velocity of fraud AND the complexity of compliance without making you pick one.
- A consolidation of risk management tools around a small handful of strategic providers.

This convergence is organizational and technological. We are increasingly seeing many banks, both Tier1 and regionals, realize that they get operational efficiency gains by merging fraud and financial crime teams under one leader. The same AI that helps detect complex fraud patterns can identify potential money laundering activity. The data that flags unusual customer behavior can surface compliance risks. A single, unified view of data that is default real-time is ultra powerful.

If you're interested in learning more about how fraud and compliance teams can collaborate more closely, read this report we put together with our friends at Fintrail.

Trend 6

Provider Market Consolidation Begins

The fraud prevention and compliance space has been fragmented, with hundreds of vendors offering point solutions. While this has driven innovation, it's also created complexity, integration challenges, and data silos.

2025 will mark the beginning of significant market consolidation in the space of fraud & fincrime risk similar to what we've seen in cybersecurity with Palo Alto Networks being acquisitive or with Wiz taking the approach of building a platform from the ground up. With Sardine, so far we have taken the approach of building. And we are seeing our competitors follow suit by merging or acquiring other players. Imitation is often the best form of flattery. We are proud that our vision that the fraud/fincrime risk space needs a new platform thought from the ground up, is resonating.

Allison Miller, CEO of Cartomancy Labs, says **increased consolidation across cybersecurity and fraud may be on the horizon**, as buyers seek solutions that address multiple threats across cyber, fraud, AML, and compliance. With rising threats and tighter budgets, she sees a growing trend of companies looking for technology that **stretches their defense dollars further** – particularly in **threat intelligence, anti-bot detection, authentication, and alerting systems** that can serve multiple use cases.

> “Companies are dealing with rising threats and tighter budgets, so they want to see where defense dollars can go further, faster. We're seeing increased demand in threat intelligence services, detection technology (anti-bot and device reputation), and alerting/review systems that can be used across cyber, fraud, AML, and compliance.”

Allison Miller
CEO, Cartomancy Labs

Organizations are increasingly seeing the value of integrated platforms that combine:

- Proprietary data at scale
- Best-in-class third-party data
- Custom ML models
- Dashboard consolidation and visualization
- AI agents for automation

Trend 7

Digital Commerce Hits Its Security Inflection Point

In 2024, bots that were traditionally the domain of “cybersecurity” became a major fraud problem. Just as the finance world has brought fraud and compliance closer, I expect we will see e-commerce, marketplaces, and platforms bring cybersecurity and fraud closer together.

2025 will be the year digital commerce fundamentally rewrites its security playbook:

- Bot detection and fraud prevention converge into unified defense systems
- Cross-platform data sharing between marketplaces, payment providers, and banks
- Traditional businesses adopt platform-level fraud prevention

The reality is stark: you can't separate payment fraud from platform abuse anymore. When a bot attack today becomes account takeover tomorrow and payment fraud next week, your defense needs to be equally integrated.

Special thanks to the Fraud Squad

This year, I reached out to some of the sharpest minds in fraud, compliance, and risk to get their perspectives on what's happening - and what's coming next. It's always a privilege to learn from people who live and breathe this work every day.

A special thanks to:

Simon Taylor

Head of Content & Strategy @ Sardine / Author of Fintech Brainfood

Simon is a leading voice in Fintech. With 20+ years in financial services, he's a renowned speaker and the creator of Fintech Brainfood, a weekly newsletter with over 30k subscribers.

Matt Vega

Chief of Staff @ Sardine

Matt Vega is a military veteran, who joined having been Director of Fraud Strategy for Novo. Matt has first-hand experience setting up Fraud & Compliance programs in banks and Fintech companies.

Christine Poulon

General Counsel @ Sardine

Christine is a specialist in Fintech and financial services law and regulatory matters. Previously Christine spent over 8 years at PayPal, before founding, then joining multiple Fintech start-ups and growth companies.

Nayeem Mano

Airbase VP, Risk & AML Compliance @ Paylocity

Nayeem has led risk analytics, payments and AML in financial institutions like ATB Financial, and Servus Credit Union, and became VP of AML, Risk and Fraud at Airbase (acquired by Paylocity).

Allison Miller

CEO @ Cartomancy Labs

Allison protects consumers from online threats. Allison was SVP Technology at Bank of America building the defensive stack, before becoming CISO and VP of Trust at online community Reddit

Sarah Mirsky-Terranova

Owner & Principal @ AE Consulting

Sarah was Head of Special Investigations Unit for BNP Paribas in New York, before leading BSA/AML with European Neobank N26, Albert and then Banking as a Service Platform Synctera. Today Sarah is a fractional compliance officer for banks, and fintech companies.

Jas Randhawa

CEO & Managing Partner @ StrategyBRIX

Jas Founded StrategyBRIX after having been Head of Financial Crime and Stripe, and Global Head of Financial Crime for Airwallex. Building on decades in EY and PwC, Jas is a specialist in where technology can be practically applied for compliance users.

Andrew Austin

Head of Fraud @ Sardine

After more than a decade in the US Miltary, Andrew joined Fifth Third Bank where he became product owner for AML Transaction Monitoring, before product managing Merchant Fraud for WorldPay, and leading Fraud Strategy at CarMax