

# Scaling AI readiness across fraud, identity, and money laundering mitigation

**Part 1: The case for an integrated fraud, identity,  
and AML response**



This is a three-part series exploring the evolving financial crime landscape and the role of AI in helping organizations respond. In part 1, we examine the growing overlap across fraud, identity, and anti-money laundering (AML).

Payments organizations have entered a period where fraud, identity, and money laundering risks are becoming increasingly interconnected. AI is accelerating the speed, scale, and sophistication of financial crime, enabling bad actors to industrialize tactics such as synthetic identities, deepfakes, phishing, and account takeover.

In response, institutions are moving beyond isolated automation efforts toward a broader redesign of data, models, investigations, governance, and operations. For payments leaders, this is not just a technology modernization agenda; it is a strategic imperative to scale AI readiness in ways that improve detection, strengthen decision-making, and support more effective, enterprise-wide mitigation of converging risks.

# The need for a more integrated approach to financial crime

AI is reshaping the financial crime landscape by accelerating the speed, scale, and complexity of threats. In 2025, the FBI's Internet Crime Complaint Center recorded 22,364 complaints with an AI-related descriptor and nearly \$893 million in associated losses, underscoring how quickly AI-enabled fraud and scams are translating into material, real-world impact.<sup>1</sup> A joint April 2026 paper from the American Bankers Association, the Better Identity Coalition, and the Financial Services Sector Coordinating Council cited a 700% rise in fintech-sector deepfake incidents, organized criminals, and nation-state actors, exploiting weaknesses across banks and fintechs, as well as health care, retailers, and government benefit programs.<sup>2</sup> Evolving risks, including AI-enabled exploitation of vulnerabilities, enable bad actors to find weak points and scale methods. Synthetic identities, deepfakes, and other AI-enabled tactics are exposing weaknesses in legacy verification, monitoring, and escalation approaches while separated signals, data, and investigative workflows are making siloed responses less effective.

At the same time, regulatory expectations are also evolving to emphasize that financial crime programs should be more agile. The Financial Crimes Enforcement Network's (FinCEN) April 2026 proposed rule reinforces this shift by encouraging the responsible use of advanced analytics and AI in compliance programs.<sup>3</sup>

Against this backdrop, institutions need an integrated approach to financial crime risk across fraud, identity, and AML. When models, data, and escalation paths are aligned, organizations are better positioned to identify connected threats earlier and respond more effectively to AI-enabled activity that cuts across traditional control boundaries.

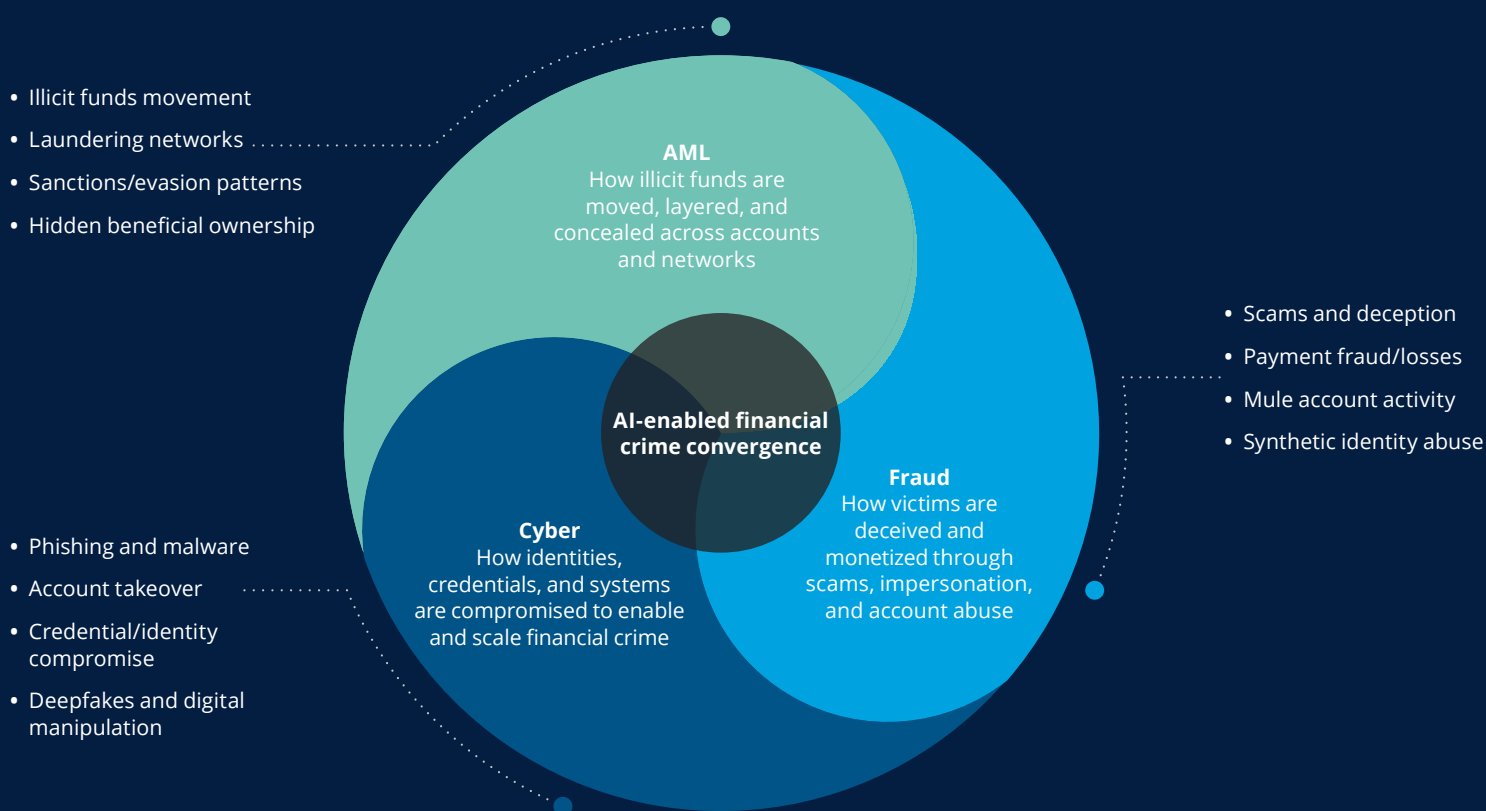
In 2025, the FBI's Internet Crime Complaint Center recorded 22,364 complaints with an AI-related descriptor and nearly \$893 million in associated losses

# Overlapping fraud, identity, and money laundering typologies

AI readiness in financial crime starts with a structural shift in the threat environment: Fraud, identity, and money laundering risks are no longer separable. Historically, these domains were managed through adjacent but distinct operating models, each with their own teams, typologies, workflows, and investigative mandates. As AI-enabled crime becomes more sophisticated,

the same actors, behaviors, and indicators surface across each of these channels. For example, FinCEN found that identity-related suspicious activity totaled \$212 billion in 2024 across 1.6 million reports and frequently involved fraud, false records, identity theft, third-party money laundering, and circumvention of verification standards.<sup>4</sup>

**Figure 1. Convergence of fraud, identity, and money laundering risks**



The overlap is especially visible in synthetic identity activity. The Deloitte Center for Financial Services projects synthetic identity fraud could generate at least \$23 billion in losses by 2030 and notes that bad actors can purchase personally identifiable information on the dark web at minimal cost, while Generative AI makes producing photo-realistic likenesses progressively cheaper.<sup>5</sup> Synthetic identities

are being used not only to open accounts or obtain credit fraudulently, but also to establish seemingly legitimate accounts that can later facilitate money movement and laundering activity. The implication for fraud and AML teams is that synthetic identity signals cannot sit only in onboarding or fraud operations but need to be shared across customer due diligence, transaction monitoring, and investigations.

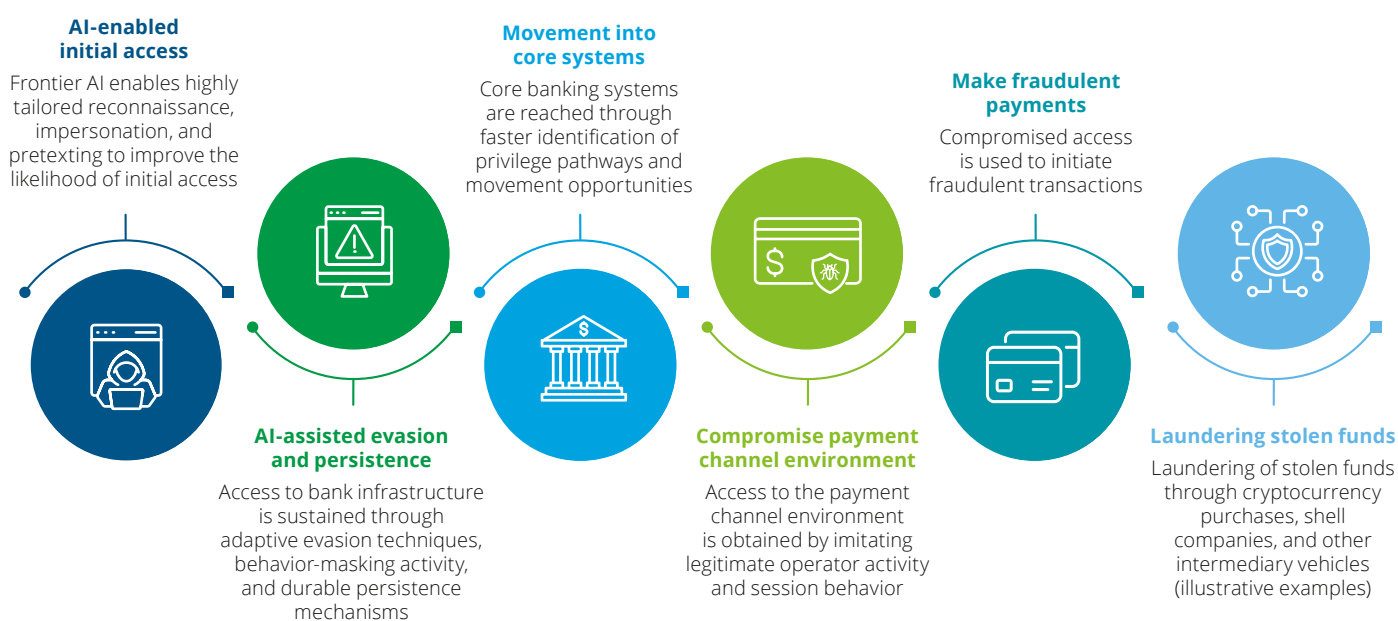
Money mules, scams, and human trafficking are increasingly becoming cross-domain risks as the same customers, accounts, and payment channels can be used to receive deceptive payment proceeds, rapidly disperse funds, and obscure the broader criminal activity behind them. Impersonation scams, authorized push-payment-style fraud, and business email compromise may begin as fraud events, but they often rely on mule accounts, third-party money movement, and coordinated networks that create clear AML relevance.

Human trafficking and related exploitation often depend on networked actors, laundering channels, and digital payments that may appear routine in isolation, but they reveal suspicious patterns when analyzed in a broader context. FinCEN reported that Bank Secrecy Act filings linked to online child sexual exploitation and human trafficking increased from 336 in 2020 to 1,975 in 2021,<sup>6</sup> and FinCEN's 2025 priorities and notices indicate these risks remain an active enforcement and AML concern.<sup>7</sup>

## Increasingly complex attack surfaces, further enabled by frontier AI

As frontier AI capabilities continue to advance and diffuse, the same underlying tools are making fraud schemes more realistic, scalable, and adaptive. The FBI has reported that criminals are using AI to generate deepfakes, clone voices, mass-produce phishing content, and automate social-engineering tactics at scale; in 2025 alone, the IC3 received 22,364 AI-enabled fraud and scam complaints.<sup>8</sup>

**Figure 2. Frontier AI-enabled financial crime attack chain**  
From initial access to illicit money movement



For fraud, AML, and cyber teams, the implication is that identity, credential, device, and entity signals should be treated as core inputs to financial-crime models, not as adjacent data owned solely by information-security functions.

## Emerging payment products increase the velocity of losses

The macro payments environment is likely to intensify these risks, with peer-to-peer, real-time payments, and stablecoins playing an increasingly important role in scam monetization and broader financial crime. Alongside digital assets, instant payments, and cross-channel payment flows, stablecoins can increase the speed, reach, and complexity of financial crime by enabling faster movement of funds across platforms and jurisdictions. The FBI

reported 181,565 cryptocurrency-related complaints in 2025, with associated losses exceeding \$11.3 billion, illustrating how digital assets can accelerate cross-border fund movement, layering activity, and the rapid transfer of proceeds tied to scams and other illicit activity.<sup>9</sup> These developments make it easier for bad actors to transfer value quickly, obscure transaction flows, and blend fraud and scam proceeds with other forms of suspicious activity.

The FBI reported 181,565  
cryptocurrency-related complaints  
in 2025, with associated losses  
exceeding \$11.3 billion



# How Deloitte can support your organization

Scaling AI across fraud and AML requires deep experience in business strategy, data, technology, operating model, and governance so that AI can be deployed effectively, responsibly, and at enterprise scale. We can help your team:

- **Define the AI operating model across fraud, identity, and AML:** Establish how AI should be deployed across adjacent fraud, identity, and AML functions, including the business objectives, governance model, decision rights, and accountability structure needed to support sustainable adoption.
- **Strengthen identity, biometrics, and cyber defenses against AI-enabled fraud:** Drawing on Deloitte's Cyber Identity, Cyber AI, and Digital Identity+ capabilities, we can help you modernize onboarding, authentication, and ongoing customer monitoring—leveraging physical and behavioral biometrics, liveness and deepfake detection, and phishing-resistant authentication.
- **Secure frontier and agentic AI deployments end to end:** Apply Deloitte's Secure Software Development Lifecycle (SSDL), Managed Extended Detection and Response (MXDR), and

AI-aware threat-modeling capabilities to harden large language models (LLMs) and autonomous agents, both internally and externally. We can help increase your defense against prompt injection, memory poisoning, tool misuse, model supply chain attacks, and excessive agency with controls extending from intent and guardrails through to runtime monitoring, red teaming, and post-deployment remediation.

- **Design a layered detection architecture:** Develop a detection stack that brings together rules, scorecards, machine learning, network analytics, and LLM-enabled workflow support. This also includes defining a platform strategy that balances enterprise consistency and vendor capabilities with institution-specific models, features, and decisioning logic.
- **Embed AI into investigative workflows:** Apply AI to triage, case summarization, evidence development, and investigator support activities to help reduce manual effort and improve consistency.

In part 2, we will look at how institutions can architect AI for better financial crime detection by combining stronger signals, more connected data, and more effective model design across fraud, identity, and AML.

## Contact us

### Satish Lalchand

Principal  
Deloitte Transactions and Business  
Analytics LLP  
[slalchand@deloitte.com](mailto:slalchand@deloitte.com)

### Brendan Maggiore

Senior Manager  
Deloitte Transactions and Business  
Analytics LLP  
[bmaggiore@deloitte.com](mailto:bmaggiore@deloitte.com)

### Anish Srivastava

Principal  
Cyber Leader for Financial Services  
Deloitte & Touche LLP  
[anissrivastava@deloitte.com](mailto:anissrivastava@deloitte.com)

### Jonathan Thomas

Senior Manager  
Deloitte Transactions and Business  
Analytics LLP  
[jthomas@deloitte.com](mailto:jthomas@deloitte.com)

### Nikhil Aggarwal

Managing Director  
Deloitte Transactions and Business  
Analytics LLP  
[nikhaggarwal@deloitte.com](mailto:nikhaggarwal@deloitte.com)

## Endnotes

1. Federal Bureau of Investigation (FBI), "[Cryptocurrency and AI scams bilk Americans of billions](#)," news release, April 6, 2026.
2. American Bankers Association, Better Identity Coalition, and Financial Services Sector Coordinating Council, [Recommendations for policymakers: Mitigating AI-powered attacks against identity and authentication](#), March 2, 2026, p. 2.
3. Financial Crimes Enforcement Network (FinCEN), "[FinCEN proposes rule to fundamentally reform financial institution programs designed to fight illicit finance](#)," news release, April 7, 2026.
4. FinCEN, "[FinCEN issues analysis of identity-related suspicious activity](#)," news release, January 9, 2024.
5. Val Srinivas, Satish Lalchand, and Jill Gregorie, "[Using biometrics to fight back against rising synthetic identity fraud](#)," *Deloitte Insights*, July 27, 2023.
6. FinCEN, "[FinCEN sees increase in BSA reporting involving the use of convertible virtual currency for online child sexual exploitation and human trafficking](#)," news release, February 13, 2024.
7. FinCEN, "[FinCEN year in review](#)," 2025.
8. FBI, "[Cryptocurrency and AI scams bilk Americans of billions](#)."
9. FBI, [2025 internet crime report](#), Internet Crime Complaint Center, April 6, 2026.



As used in this publication, 'Deloitte' means Deloitte & Touche LLP, which provides audit, assurance, and risk and financial advisory services; and Deloitte Transactions and Business Analytics LLP, which provides eDiscovery, analytics, and a wide range of advisory and analytic services. These entities are separate subsidiaries of Deloitte LLP. Please see [www.deloitte.com/us/about](http://www.deloitte.com/us/about) for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.

This article contains general information only and Deloitte is not, by means of this article, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This article is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor. Deloitte shall not be responsible for any loss sustained by any person who relies on this article..