2026 Wealth and Asset Management Fraud Insights Point of View

Third edition

The better the question. The better the answer. The better the world works.

Shape the future with confidence

Table of contents

1 A letter from Walid Raad

As the wealth and asset management (WAM) landscape evolves, the challenge of preventing and detecting fraud intensifies. Ernst & Young LLP (EY US) continues its vital dialogue with industry leaders through the 2026 WAM Fraud Insights Point of View (POV), shedding light on how firms are responding to the ongoing surge in fraudulent activity. This third edition builds on previous insights offering a fresh look at emerging trends and innovative strategies shaping the future of fraud prevention.

In this report, we delve into the increasing sophistication of scams, the necessity of effective categorization frameworks and the strategic investments firms are making in advanced detection technologies. We also highlight how organizations are harnessing artificial intelligence (AI) to boost operational efficiency and are employing proactive measures like red teaming to strengthen their defenses. This POV aims to tackle these pressing issues and provide valuable insights to help firms navigate the complexities of fraud in today's dynamic environment.

Walid Raad
US Forensics Financial Services Leader

2 Introduction

Consumer fraud continues to be a growing threat, with the Federal Trade Commission (FTC) reporting that customers lost more than **US$12.5 billion** in 2024[1], a stunning **25%** increase from the previous year. Investment scams alone accounted for **US$5.7 billion** in losses, reflecting a **24%** increase. At this rate, 2026 losses are on track to exceed **US$19 billion**.[2]

This surge in fraudulent activity has raised alarms among regulators and governments worldwide, prompting a wave of enforcement actions against financial institutions that may not be doing enough to protect their customers. With all signs pointing to continued growth in fraud into 2026 and beyond, the urgency for WAM firms to bolster their defenses has never been greater.

Responding to the challenge

EY US published our first WAM Fraud Insights POV in 2022, offering a detailed examination of how WAM firms were addressing fraud challenges largely stemming from the increased volumes experienced post-pandemic. The 2024 edition built on this foundation, incorporating insights from both new and returning interview respondents to highlight significant market shifts and evolving fraud strategies.

In this third edition, we delve deeper into the fraud trends of the past year, exploring fresh topics and strategies that are top of mind for WAM firms. Our team interviewed more than 20 fraud and enterprise risk management executives to gather insights from WAM firms managing assets ranging from **US$1 trillion** to **US$10 trillion**.

As fraud is not a new issue, WAM firms have made significant headway in enhancing their preventive and detective frameworks. The 2026 edition reports a **22%** decrease in average case volume compared with our 2024 iteration. While the average number of successful fraud events has decreased for our participants, they also reported a striking **74%** increase in average losses. This demonstrates that fraudsters continue to adapt their approaches and are becoming more efficient, taking more funds with fewer attempts.

As consumer fraud evolves, it's crucial to understand the key issues affecting our participants this year. Below, explore these concerns alongside industry-leading practices that effectively mitigate fraud exposure and strengthen both preventive and detection efforts.

Note: Because of the availability of data, not all respondents could answer every question. The percentages in this POV were calculated based on only the responses that were received (i.e., all results will be displayed out of 100%, with 100% representing only answers that were received).

1. Federal Trade Commission. 2025. "New FTC Data Show a Big Jump in Reported Losses to Fraud to $12.5 Billion 2024." Federal Trade Commission. March 10, 2025. https://www.ftc.gov/news-events/news/press
2. Ibid

3 Key themes in fraud trends

The increasing level of sophistication of scams continues to present a significant challenge for both institutions and their customers. The activity can be authorized by the customer, which has led to the absence of traditional red flags. Respondents indicated that this has complicated detection and prevention efforts and has made it difficult to determine the customer's true intent. As such, firms are continuing to assess their programs and seek innovative solutions to identify when customers are falling victim to scams, all while balancing the need to minimize customer friction.

Respondents are actively implementing or planning to enhance their categorization of scams. Many firms are leveraging guidelines released by the Federal Reserve as a baseline for their categorization frameworks. Categorizing scams based on these guidelines allows firms to employ targeted prevention techniques, tailor educational and awareness campaigns and identify threat vectors based on the types of scams most prevalent to the organization and its customers.

Firms are working to determine the best ways to use AI in their fraud prevention organizations by exploring relevant use cases. Most respondents are working to identify effective use cases for AI and looking for ways to maximize their return on investment (ROI). Currently, many firms are leveraging AI to assist with administrative tasks, such as generating case summaries and enhancing transactional and behavioral risk assessments. This shift results in leaner and more efficient fraud prevention organizations, while increasing service delivery to adhere to tight regulatory timeline requirements and compliance objectives.

Red teaming is a leading practice that top firms are utilizing to identify vulnerabilities in their fraud prevention organization. Some respondents have orchestrated simulated attacks and vulnerability assessments to proactively identify weaknesses in their fraud prevention measures. This has allowed industry-leading firms to strengthen their defenses by addressing potential vulnerabilities before they can be exploited by actual fraudsters.

Key investments in the past year have concentrated on improved detection capabilities. Most respondents have engaged external vendors to implement enhanced detection methods, focusing on risk orchestration, behavioral biometrics and anomaly detection. Firms have also specifically adopted biometric defenses to combat the rising threat of AI deepfakes.

The evolving fraud landscape

The rapid pace of digital innovation and the widespread adoption of AI have given fraudsters new tools to craft increasingly sophisticated schemes targeting financial institutions and their customers. For WAM firms, this evolving landscape presents significant challenges. Recent discussions with industry leaders reveal that the top three fraud threats impacting these firms are scams, account takeovers (ATO) and wire fraud. Scams have emerged as the most prevalent threat, cited by **89%** of respondents, while ATO and wire fraud were identified by **67%** and **56%**, respectively. These findings mirror insights from the previous edition of the POV published in May 2024, which similarly highlighted scams and ATO as top risks.

The challenge of scams and authorized payment fraud

Scams pose a unique challenge, especially as authorized payment fraud becomes more common. This trend complicates detection efforts, as traditional red flags often fail to signal potential issues. With authorized payment fraud, transactions are frequently approved by the customer, blurring the lines between legitimate activity and fraudulent behavior. Industry executives have noted how this complicates prevention and detection efforts; when customers authorize transactions, the absence of warning signs makes it tough to catch fraud before it happens.

Adding to the complexity is the rising concern over money mule accounts—where unsuspecting individuals are used to facilitate fraudulent transactions. These accounts have become a top priority for firms, as they can be difficult to trace and often lead to significant financial losses.
To tackle these challenges, WAM firms are actively exploring innovative solutions that can help determine customer intent and identify potentially fraudulent activities before any money changes hands.

WAM firms face rising stakes

In fiscal year 2023, respondents reported an average loss of around **US$18 million** due to successful fraud incidents, with individual losses ranging from **US$750,000** to a jaw-dropping **US$40 million**. While fiscal year 2024 shows a slight decrease in average losses to about **US$14.5 million**, the range of reported losses has expanded dramatically, with some firms facing totals as high as **US$50 million**.

As these figures illustrate, the stakes are incredibly high. WAM firms must not only contend with the evolving tactics of fraudsters but also reassess their strategies to safeguard against these escalating threats. Understanding the full scope of these challenges is essential for developing effective responses that can protect both the firms and their customers.

Investment scams: A growing threat

One significant threat highlighted by respondents is investment scams, particularly the notorious "pig butchering" schemes. These scams typically start with unsolicited outreach through social media, dating apps or messaging platforms, where fraudsters pose as wealthy investors or romantic interests. Using targeted social engineering, AI-generated identities and emotional manipulation, they build trust over time before presenting fake investment opportunities, often involving cryptocurrency or foreign exchange markets.

Account takeover: A stark reality

The challenges of ATO and scams are mounting, with **67%** of respondents noting that these types of fraud have seen the highest increase in volume. Fraudsters are increasingly using social engineering tactics and malware to breach client accounts. Once inside, they swiftly initiate unauthorized transactions—such as wire transfers and peer-to-peer payments—often before any alerts or controls can kick in.

Wire fraud has been particularly problematic for respondents over the past year, given the rapid movement of funds and the difficulty in recovering lost money. This issue is especially relevant for WAM firms, which frequently oversee large transfers for investments, capital calls and client disbursements. Respondents reported a rise in fraudulent activity linked to intercepted capital calls, where fraudsters altered wire details and banking information, diverting funds to fraudulent recipients.

A shift to manual fraud

However, as firms enhance their controls against advanced technologies, some respondents have noticed a troubling shift back to more manual fraud methods. Check fraud emerged as a top concern for **44%** of respondents, encompassing stolen, whitewashed and counterfeit checks. Some firms even reported fraudsters using fax communications to conduct their schemes.

New fraud threats on the horizon

The past year has also seen the rise of new threats, including an uptick in securities and trading fraud, primarily involving initial public offerings (IPOs) and "pump-and-dump" schemes that involve artificially inflating the price of an owned stock through false and misleading positive statements (pump), in order to sell the cheaply purchased stock at a higher price (dump).

One respondent noted that more than **70%** of their ATO cases were linked to trading fraud, where fraudsters gain access to victims' accounts to conduct unauthorized trades and manipulate the market. These schemes highlight the critical need for real-time transaction monitoring and robust authentication measures to safeguard client accounts.

As fraudsters continue to merge traditional tactics with innovative technologies, WAM firms must stay alert. Investing in advanced detection capabilities and prioritizing customer education will be essential to mitigate risks in this increasingly complex fraud landscape.

Elder abuse

As the industry confronts the rising tide of elder abuse, implementing a multifaceted approach that integrates behavioral insights, community engagement and proactive measures is essential. Recognizing that the unique behaviors of older clients is crucial for identifying potential fraud, firms are increasingly focusing on behavioral analytics and monitoring. A significant **78%** of firms are utilizing risk signals—such as behavioral changes or sudden account modifications—as critical red flags for elder abuse.

To further safeguard older clients, **100%** of respondents have adopted a trusted contact model. This model requests that clients have a reliable point of contact for assistance that institutions can reach out to if they suspect fraud. Additionally, WAM firms are enhancing education efforts by providing scam alerts, training and regular communications to raise awareness about potential threats. This proactive approach empowers clients and equips investment advisors with the knowledge to recognize and respond to signs of elder abuse.

Leading practices for elder fraud prevention

Establishing internal "pause points" for verification on suspect transactions allows for additional scrutiny, reducing the likelihood of fraud. Observing client interactions, for example, who speaks, who decides, and how clients behave, can also provide valuable insights into potential fraud. In addition, simplifying communication and verification steps for seniors helps them navigate their financial interactions confidently. Incorporating reflective questions before executing large payments can serve as a safeguard against impulsive decisions. By combining transaction data with behavioral cues, such as time of day and unusual spending patterns, firms can identify potential elder fraud early.

The need for cross-sector collaboration

Addressing elder abuse requires coordinated action among banks, Adult Protective Services (APS) and law enforcement. Relationship advisors play a vital role as the first line of defense against elder fraud, emphasizing that red flags are often behavioral rather than transactional. Sudden changes, such as new cosigners, or clients showing undue deference to a "helper," can indicate potential issues that warrant further investigation. Understanding the emotional complexities faced by victims is also essential. Many older individuals fear confrontation, loss of independence and embarrassment, especially when family members are involved. This sensitivity can guide frontline employees in approaching situations with care.

Insider threats

As organizations focus on fraud threats from within, our respondents are united in their commitment to robust insider threat risk management programs.

Although there's consensus on the need for vigilance in preventing and detecting these threats, the methods for managing insider risk vary significantly across firms. All respondents have established a formal insider threat risk program, with a notable **25%** increase in firms leveraging other business units for prevention and detection. Specifically, **55%** of firms integrate insider risk responsibilities into broader risk or cybersecurity frameworks, highlighting the crucial role of cybersecurity in identifying insider threats. Thirty-four percent of respondents manage these threats primarily through investigations, fraud escalation or risk-led oversight, with another **11%** involving legal departments in their processes.

These diverse approaches underscore a growing recognition of the overlaps between insider threats, compliance, cybersecurity and fraud. Most firms have adopted either a fusion model of collaboration or centralized risk ownership, characterized by multiline oversight, cross-functional coordination and enhanced governance integration, or are increasing collaboration among fraud, anti-money laundering (AML) and cybersecurity teams.

However, despite the consensus on the importance of proactive detection, just **63%** of respondents provided clear sources for escalating insider threats, signaling a need to refine reporting processes. Among those, **87%** utilize various business units that interact directly with insider threats to escalate incidents. Key departments involved in this escalation include cybersecurity, compliance and corporate security, while the remaining **13%** rely on integrity hotlines and chatbots for monitoring.

In summary, while firms are making strides in managing insider threats, a unified and coordinated approach is essential. By fostering cross-functional collaboration and refining escalation processes, organizations can strengthen their defenses against insider risks and better safeguard their assets.

4 The future of fraud

EY US team's point of view

Based on extensive conversations with industry participants and an analysis of leading fraud detection and prevention strategies, one conclusion that we offer is clear: **Firms must adopt proactive measures to protect themselves and their clients from an ever-evolving threat landscape. Our recommendations include:**

Refining categorization frameworks

As authorized payment fraud rises, firms need to refine their categorization frameworks and establish clear accountability for customers who fall victim to scams. By leveraging guidelines from the Federal Reserve, the industry can align on handling litigation related to scams and elder exploitation. The distinction between unauthorized and authorized payment fraud will increasingly determine whether firms reimburse customers, with a growing trend toward denying reimbursement if a customer has authorized any account access or payments in any form.

Integrating AI into fraud prevention

Firms are also capitalizing on the integration of AI into their fraud prevention efforts. As AI becomes more prevalent, organizations are moving beyond automating routine tasks to implementing advanced strategies. Industry leaders are beginning to adopt capabilities such as behavioral and transactional risk assessments, automated investigation processes and machine learning to identify trends in large data sets. This long-term adoption of AI is essential for improving efficiency in fraud investigations.

Enhancing authentication and verification

To combat sophisticated fraud tactics such as AI-generated deepfakes and synthetic identities, firms must improve their authentication and verification methods. Traditional techniques, such as one-time passwords and voice recognition authentication are no longer sufficient. Instead, firms should transition to advanced strategies, including step-up authentication tailored to specific risk factors and the use of behavioral biometrics. Continuous evaluation of these methods is crucial to balance security with a smooth customer experience.

Integrating fraud risk management

Firms should prioritize integrating fraud risk management across their organizations to improve communication and collaboration among relevant business units. Respondents have noted significant challenges related to fraud risk governance and existing silos. A coordinated approach can enhance fraud prevention and detection, providing a comprehensive understanding of risks and vulnerabilities. A notable trend is the establishment of fraud fusion centers, which align operations, such as fraud prevention and AML, to create efficiencies and better understand the financial crimes impacting the business.

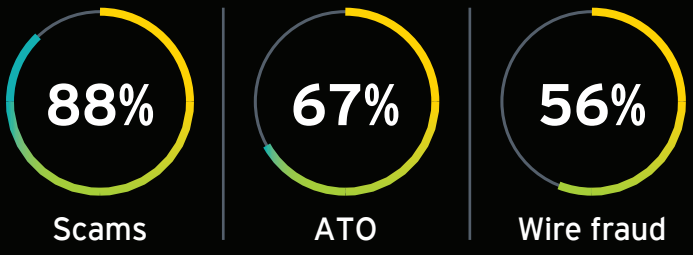
In summary, as firms navigate the complexities of fraud, adopting these recommendations will be critical. By refining categorization frameworks, integrating AI, enhancing authentication and verification methods and fostering cross-functional collaboration, organizations can strengthen their defenses against fraud and better protect their clients.

Key 5 takeaways

The increasing level of sophistication in fraud

Top three current fraud threats

Based on discussions with respondents, the top three current fraud threats impacting firms in the WAM sector were scams, ATO, and wire fraud. Scams emerged as the most prevalent threat, cited by **88%** of respondents, while ATO and wire fraud were identified by **67%** and **56%** of respondents, respectively. These findings were consistent with the insights published in the 2024 edition of the Wealth and Asset Management Fraud Insights POV, which similarly highlighted scams and ATO as top risks for WAM organizations.



The acceleration of digital innovation and widespread adoption of AI have empowered fraudsters to deploy increasingly complex schemes that target both firms and their customers. Respondents reported challenges with business email compromise **(14%)** and impersonation scams **(17%)**, driven by the abundance of publicly available information and the use of deepfake technologies to bypass internal controls.

Scams

Scams pose a unique challenge for firms, as authorized payment fraud is becoming more common, making it more difficult to detect through conventional red flags and limiting the effectiveness of existing controls. Sixty-seven percent **(67%)** of respondents report persistent fraud challenges with ATO and scams.

Evolving fraud tactics have been augmented with the use of new technologies, to both increase the reach and speed at which fraudsters can act. WAM firms have responded, developing more robust controls that more effectively and efficiently identify these new red flags.

Some fraudsters, in turn, have reverted to more traditional, manual methods, thereby avoiding these control enhancements and are expanding opportunities to defraud customers with both new and older technologies. More specifically, check fraud continues to be a major threat, cited by **44%** of executives interviewed, including stolen, whitewashed and counterfeit checks.

New and evolving fraud threats

This past year saw the emergence of new and evolving threats, such as an increase in securities and trading fraud, mainly involving IPOs and pump-and-dump schemes. One respondent stated that more than **70%** of their ATO cases involved trading fraud, where fraudsters gain access to victim accounts and conduct unauthorized trading to manipulate the market.

Categorization of scams

In 2024, only **25%** of respondents interviewed categorized scams by specific typologies, but this year, that figure has surged to **78%**, better allowing them to identify trends in tactics leveraged by fraudsters. By distinguishing between ATO fraud and other scam types, firms are enhancing their scam tracking capabilities and updating fraud case management systems to include detailed subcategories, allowing firms to capture comprehensive data on prevalent scam techniques, directing resources more effectively and refining preventive measures. Leading firms are adopting guidelines from the Federal Reserve to enhance their categorization frameworks, targeting prevention strategies and educational campaigns.

EY US has released a four-part scams POV series aimed at addressing critical aspects of regulatory action, categorization benefits, and useful tips to identify red flags and strategies for fraud liability mitigation.

With scams continuing to rise, this series is designed to assist firms in navigating the balance between compliance and consumer protection. The POV series is a resource for firms seeking to enhance their understanding of regulatory requirements and improve consumer protection measures. By providing actionable insights and practical guidance, EY US aims to empower organizations to navigate the regulatory landscape with confidence and integrity.

PART 1

Analyzing the current state of fraud scams

▶ View

PART 3

Scam prevention: spotting red flags to mitigate losses

▶ View

PART 2

Scams: the impact of detailed categorization

▶ View

PART 4

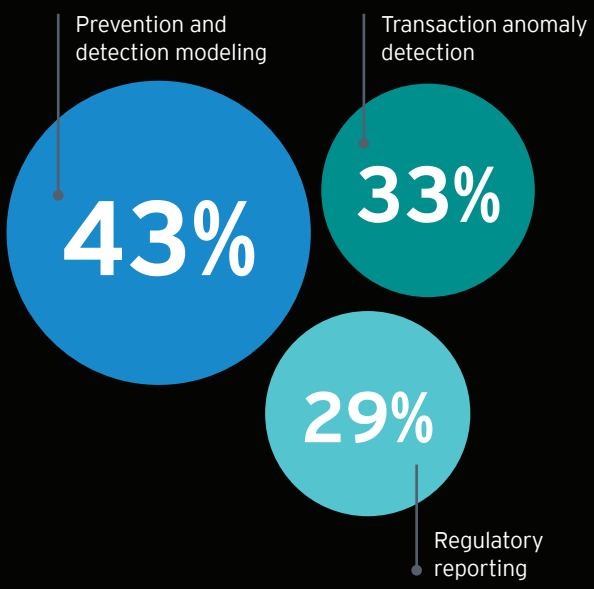
Scams: Mitigate liability for losses

▶ View

Technology: AI integration

All respondents are leveraging AI to some degree within their fraud prevention organization, from enhancing regulatory reporting to detecting transaction anomalies.

Most common uses for AI



Industry leaders have implemented AI in fine-tuning their existing fraud prevention and detection models and rules **(43%)** as well as for transaction anomaly detection **(33%)**, and for regulatory reporting **(29%)**.

Concurrently, experimentation with generative AI (GenAI) is gaining traction, with half of respondents **(50%)** noting that they are exploring use cases for monitoring and incident analysis, among other scenarios.

Many organizations are also implementing either in-house models or adopting vendor solutions, focusing on automation and regular model updates to minimize errors and boost efficiency. Firms are also increasingly using specialized vendor tools to address specific fraud typologies, including check, Automated Clearing House (ACH) and wire fraud. Interestingly, while AI is enhancing the efficiency of fraudsters, some respondents **(43%)** reported that the nature of fraud threats has not significantly changed, as most fraudsters are leveraging new tools and altered approaches to execute familiar schemes rather than executing entirely new types of fraud.

Technology: Digital assets and cryptocurrency

The current trends among respondents regarding their risk appetite and policies for digital assets and cryptocurrency reveal a predominantly cautious approach. All respondents **(100%)** exhibit a low-risk appetite, opting to avoid direct interactions with cryptocurrencies. As a result, they typically do not permit customers to hold or transact in crypto directly and noted there were no plans to change course in the foreseeable future. Currently, participant involvement in digital assets is largely confined to exchange-traded funds (ETFs) or managed funds **(71%)**, with some firms beginning to monitor wallets and evaluate payments to digital asset firms to identify potential scams.

Fourteen percent of respondents noted that they use a third-party vendor to enhance their digital asset capabilities. In addition, monitoring and evaluation efforts are emerging, as some firms begin to track wallets and evaluate payments to digital asset firms to identify potential scams.

Overall, as firms explore the possibility of offering crypto-related products, they are looking to upgrade their existing controls and develop new controls, highlighting the importance of robust risk management frameworks that can effectively address the unique challenges and regulatory requirements associated with digital assets.

In fiscal year 2023, participants experienced an average of approximately **US $18 million** in losses from successful fraud incidents. Reported losses ranged from **US$750,000 to over US$40 million**.

In fiscal year 2024, participants experienced average fraud losses of approximately **US$14.5 million**. This year also showed substantial variances in total fraud losses, with responses ranging from approximately **US$900,000** to as high as **US$50 million**.

Fraud loss metrics

Realized fraud losses in fiscal year 2023 and fiscal year 2024 varied significantly across respondents with **62.5%** of firms reporting under **US$5 million** in fraud losses in 2024 and **37.5%** of firms reporting over **US$25 million** in fraud losses in 2024. It's worth noting that **33%** of respondents displayed a decrease in fraud losses from 2023 to 2024.

Loss recognition and valuation

Multiple respondents provided differing views of loss recognition and valuation, noting different methods of defining fraud, tracking fraud and recognizing fraud losses that impact measurements. For example, some firms value fraud losses at incident inception, while others value fraud after completing an investigation. Even where primary cost calculations align, many secondary costs are generally not included in cost calculations, such as litigation, regulatory and operational costs, making fraud losses likely larger than reported.

New account fraud

A distinct finding from this year's respondents was the significant volume of new account fraud (NAF). This case type was the highest average case volume **(5,240)** and third highest value of loss amount **(US$4,050,000)** across all respondents.

Scam cases and SARs

Of the different fraud types presented, scams accounted for the second highest average case type by volume **(2,444)**; however, scams presented the highest average loss amount **(US$8,620,000)** per respondent. Additional respondent data also suggested a strong correlation between scam cases and suspicious activity reports (SARs) and high customer losses.

Significant ATO activity

Across respondents, ATO cases were the third largest average case type by volume **(1,242 cases)** and second largest average loss amount.

The fraud prevention organization: alignment

The fraud prevention organization was mostly aligned with either the compliance function **(34%)** or within risk **(33%)**. The remaining respondents noted that they align the organization with the cyber or technology functions.

While there is no one correct way to set up a fraud prevention organization, there are benefits to each of these options. Aligning a firm's fraud prevention organization with its risk management function enhances holistic risk assessment and resource allocation, enabling a comprehensive approach to identify and mitigate various risks. When integrated with the compliance organization, fraud prevention promotes adherence to regulatory requirements while streamlining reporting and investigations and fostering a culture of accountability. Meanwhile, aligning with the cybersecurity function allows for a unified strategy against interconnected threats, enhancing data protection and incident response capabilities.

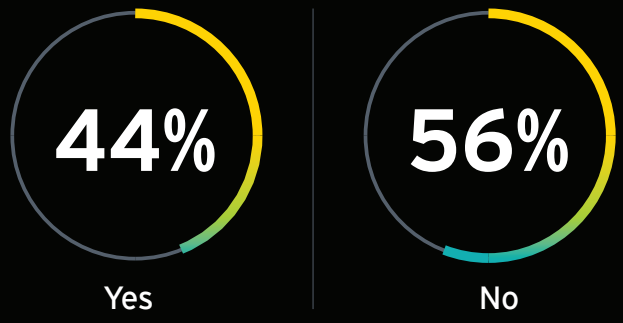
Each alignment not only strengthens the institution's defenses against financial crimes but also promotes operational efficiency and regulatory compliance, ultimately safeguarding assets and reputation. Regardless of where the fraud prevention organization is positioned, it is essential for firms to coordinate fraud management and detection functions with other stakeholders responsible for implementing the company's strategies and procedures for fraud prevention, detection and operational efficiency.

An overwhelming majority **(85%)** of respondents maintain the management of identity and authentication under the Chief Information Security Officer (CISO) or the broader cybersecurity function.

In this structure, fraud teams often take ownership of the processes related to fraud detection and prevention, while the technology and controls necessary for secure authentication are managed by cybersecurity professionals.

Collaboration and adopting a fusion center

Firms integrating fraud and AML into a fusion center



Although industry-leading firms have taken the step to combine their fraud and AML functions into a single group of fusion center **(44%)**, most respondents indicated that they do not have plans to alter their formal organizational structures **(56%)**.

They are, however, increasing the collaboration among fraud, AML and cybersecurity teams, highlighting the importance of cohesive strategies in addressing complex financial crimes—leveraging all available information across the organization while optimizing operational effectiveness. Respondents noted that they are moving towards shared case management, workflow integration, data sharing opportunities and process alignment, with the goal of reducing duplication of efforts and enhancing efficiency.

Fraud mitigation strategies

Challenges and strategic initiatives

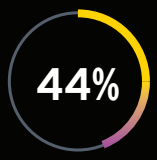
The predominant challenge identified by respondents **(50%)** was determining the most effective way to implement AI and adapt to technological advancements as fraud continues to evolve. Many firms are actively analyzing their strategies for leveraging AI in fraud detection and prevention and collaborating with third-party vendors to enhance these capabilities.

Respondents **(44%)** also highlighted challenges related to their global operating model and the alignment of the entire organization on fraud risk management. While the organizational structures among participants varied significantly, nearly all firms recognized the necessity of collaboration across business units to effectively prevent and detect fraud and assess threats.

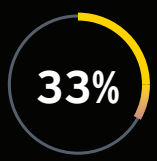
Determining customer intent and responding to the rise of authorized payment fraud is another challenge confronting WAM firms. Thirty-three percent **(33%)** of participants noted it is becoming increasingly difficult to prevent and detect fraud when the transactions are being authorized by the customer, leading to an absence of traditional red flags.

Additionally, the increased risk of money mule accounts has become top of mind for firms in the industry. As such, firms are exploring innovative solutions to determine customer intent and to identify potentially fraudulent activities before money movement can occur.

of respondents indicated that determining the most effective way to implement AI was a challenge.



of respondents indicated challenges around their global operating model.



of respondents indicated that they were facing challenges in determining customer intent and responding to the rise of authorized payment fraud.

Mitigation strategies

To effectively address challenges facing fraud prevention organizations, firms have made significant investments and implemented new strategic initiatives over the past year. Several firms **(50%)** have specifically directed their investments toward advanced identity verification tools and synthetic ID detection systems, including imposter detection and identity theft tools, to enhance their preventative control framework.

Additionally, many firms **(50%)** are focused on enhancing their detection methods by shifting to a proactive approach that includes implementing login and transaction anomaly detection and behavioral biometrics. To combat the rise in deepfakes, many firms have adopted biometric defenses to identify AI-generated voices in call center interactions. Lastly, firms have consistently leveraged transaction monitoring to identify emerging fraud trends and enable real-time analysis of transactions to identify suspicious activities.

Seeking balance

As firms strive to adopt a more proactive approach to fraud prevention and detection, evaluating the balance between user experience and security in fraud prevention measures has been top of mind for respondents this year. As such, the majority of respondents **(62%)** have orchestration platforms in place that can adapt customer friction based on real-time risk monitoring.

This industry-leading practice allows transactions to be stopped in real time and a manual review to be conducted if red flags are present while maintaining low customer friction. Maintaining this balance is becoming increasingly crucial for firms to safeguard customers from losses while fostering a user experience that encourages retention.

Elder abuse and litigation

In the evolving landscape of elder abuse, **100%** of respondents are placing an increased focus on age-based behavioral analytics and monitoring. This shift recognizes that understanding the unique behaviors of older customers is essential in identifying potential fraud.

Seventy-eight percent of firms are utilizing risk signals, such as behavioral changes or sudden account changes by older customers, which serve as critical red flags in elder abuse. In addition, **100%** of firms have implemented the use of a trusted contact model, requesting that older customers have a reliable point of contact for assistance and guidance along with a key point of contact for institutions to contact should they suspect fraud.

Enhanced education efforts for both customers and investment advisors are also prevalent, as **100%** of participant firms actively provide scam alerts, training and regular communications to raise awareness about potential threats to their older customers. This proactive approach not only empowers customers but also equips investment advisors with the knowledge needed to recognize and respond to signs of elder abuse.

Insider threats

With the continued focus on fraud threats originating from within the organization, all respondents **(100%)** expressed their unified commitment to maintain a robust insider threat risk management program. While the need to stay vigilant in preventing and detecting insider threats was universally agreed upon, the way in which insider risk is managed throughout the participants' organizations did vary.

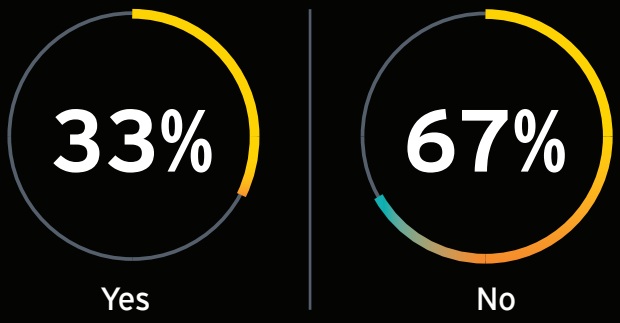
Similar to prior years, all respondents had formal insider threat programs with different approaches to address program responsibility and oversight. This year saw a **25%** increase in firms leveraging other business units to assist in insider threat prevention and detection. One common business unit utilized to combat insider risk was cybersecurity. For example, **63%** of participants placed insider risk responsibilities alongside broader risk or cybersecurity frameworks. Other business units mentioned in the process of tackling insider threats included legal departments and internal investigations.

All respondents **(100%)** noted risk overlaps with insider risk, with most adopting either a fusion model of collaboration or centralized risk ownership. Common traits behind these approaches typically include multiline oversight, cross-functional coordination and increased governance integration.

However, while there is consensus on the importance of proactively detecting insider threats, just **63%** of participants provided definitive sources from which their organization escalates insider threats, showing a continued need to further refine related reporting processes. Of these respondents, **89%** noted using various business units with direct interaction with insider threats to escalate incidents.

Red teaming practices

Firms conducting formal fraud-focused red teaming exercises



Although red teaming exercises deliver measurable benefits such as fraud loss reduction, improved regulatory alignment and enhanced customer trust, the majority of respondents **(67%)** have not conducted fraud-focused red teaming exercises. Instead they rely on alternative methods such as vulnerability testing and scenario analysis. Several organizations noted that fraud is often addressed indirectly through broader cyber or sanctions-related testing.

While some organizations are beginning to embrace fraud red teaming, its adoption among WAM firms remains limited compared with broader industry practices. Firms that rely solely on tabletop exercises or cyber-focused assessments may be more vulnerable to fraud, as they often overlook critical fraud-specific weaknesses in customer-facing processes and nontechnical functions.

Organizations can move beyond theoretical exercises and adopt intelligence-driven fraud red teaming to validate control effectiveness, identify gaps and prepare for emerging threats. Those already engaged with fraud red teaming exercises set a strong example by integrating fraud into their broader programs and continuously updating scenarios based on threat intelligence.

Authentication and identity verification

Consistent with the previous edition of the POV, the customer authentication process has remained top of mind. The rise of AI impersonation scams and data leaks has challenged WAM firms to consistently look for improved methods to authenticate their customers. As such, firms have continued to move away from traditional authentication methods, such as voice biometrics and knowledge-based authentication (KBA). These tactics have proven to be ineffective due to the emergence of AI-generated deepfakes, as well as the widespread availability of personally identifiable information (PII) exploited by bad actors.

The majority of participants **(67%)** employ multifactor authentication as a standard practice, often mandating it for customer logins. Many firms **(56%)** utilize one-time passwords (OTP) as a form of multifactor authentication, though there is growing concern about becoming overly reliant on this method, as modern attack techniques have become very effective at bypassing them. Consequently, **78%** of participants are either exploring or have already implemented more robust authentication methods, including app-based authentication, hard and soft tokens and selfie verification for digital accounts. To address high-risk cases, some firms even require in-person verification.

In addition, many firms within the industry are pushing to digitize the identity verification process and improve the utilization of existing technologies for facial and ID scanning to confirm user identity.

Customer identification

For the majority of respondents, customer identification, source of wealth and customer intent are verified as part of the customer identification program (CIP). If red flags are present, firms require the customer to provide supporting documentation (e.g., a government ID) to verify any unsubstantiated information. When a high-risk account is identified, **38%** of respondents perform enhanced due diligence and negative news searches. And to combat customer misrepresentation and potential mule accounts, industry-leading firms verify the source of funds and account purpose during the account opening process.

As money mule accounts become more prevalent across the industry, many firms are proactively taking steps to mitigate the associated risks. Firms have implemented a variety of preventative measures, including restricting online account openings, implementing deposit holds, and partnering with third-party vendors to enhance transaction screening with verification activities such as confirming ownership of external bank accounts and conducting online account verification.

Partnering with external vendors can lead to improved accuracy and a reduction in false positives due to their access to comprehensive data sources and streamlined processes. Additionally, utilizing external vendors can reduce the administrative burden on fraud organizations and offer cost savings as opposed to maintaining in-house capabilities.

6 Characterizing fraud

Evolving strategies and accountability

As authorized payment fraud continues to rise, WAM firms are stepping up their game by refining their categorization frameworks and establishing clearer accountability for customers who fall victim to scams. With the Federal Reserve guidelines serving as a foundational baseline, the industry is aligning more closely on how to handle litigation stemming from scams and elder exploitation. This shift is particularly important as the distinction between unauthorized and authorized payment fraud becomes crucial in determining whether firms will reimburse customers who have been scammed. If a customer has authorized any account access or payments, reimbursement may not be on the table.

A significant shift in scam tracking

In the previous edition of the POV, just **25%** of respondents were actively categorizing scams. Fast forward to this year, and a remarkable **78%** of respondents are now improving their scam-tracking capabilities. This dramatic shift reflects a growing recognition of the need for robust fraud management systems. Firms are updating their fraud case management systems to include detailed subcategories for scams, distinguishing between ATO fraud and other types of scams.

Today, most firms categorize scams into primary groups such as investment, romance and tech scams. They are also focused on tracking whether the fraud originated from an authorized payment, as this directly impacts reimbursement decisions. By capturing detailed information on prevalent scam techniques, organizations can better direct resources and refine their preventive and detective controls.

Tools for mitigation

Leading WAM firms are leveraging the Federal Reserve guidelines to target prevention techniques, tailor educational campaigns and identify the most pressing threat vectors. The guidelines for classifying fraud include valuable toolkits designed to enhance understanding and response strategies.[3] The initial release of the Scams Mitigation Toolkit and Check Fraud Mitigation Toolkit focused on building foundational knowledge about different types of scams and check fraud. These resources probed into the tactics and human vulnerabilities that often enable fraud to succeed, as well as common scenarios that financial institutions, service providers and individuals may encounter.

By utilizing these toolkits, firms can not only improve their categorization efforts but also empower their teams to recognize and combat fraud more effectively. As the fraud landscape continues to evolve, staying informed and proactive is essential for safeguarding both WAM firms and their customers. And as the industry adapts to the complexities of fraud, the emphasis on categorization, accountability and education will be key in mitigating risks and in enhancing customer protection.

3. FedPayments Improvement. 2026. "About the FraudClassifier Model | FedPayments Improvement." FedPayments Improvement. February 19, 2026. https://fedpaymentsimprovement.org/strategic-initiatives/payments-security/fraudclassifier-model/

7 Fraud mitigation

Staying ahead of fraud: investments in detection capabilities

WAM firms are heavily investing in detection capabilities to combat fraud. Over the past year, many organizations have turned to external vendors to implement advanced detection methods, with a particular focus on behavioral biometrics and anomaly detection. These technologies are essential as fraudsters become more sophisticated, employing tactics such as AI-generated deepfakes and synthetic identities (artificially created identities that combine real and fictitious information).

Proactive detection strategies

Many organizations are enhancing their detection methods by implementing login and transaction anomaly detection, as well as wire fraud detection systems. By focusing on behavioral biometrics, firms can spot unusual patterns that may indicate fraudulent activity.

Additionally, to combat the rise of deepfakes, many firms have adopted biometric defenses capable of recognizing AI-generated voices during call center interactions. This multilayered approach is crucial for maintaining robust security. However, conventional transaction monitoring remains a cornerstone of fraud detection, enabling firms to identify emerging fraud trends and conduct real-time transaction analysis.

The need for advanced authentication

Traditional authentication methods, such as one-time passwords and voice recognition authentication, are losing their effectiveness in the evolving fraud landscape. As fraudsters get smarter, firms must adopt more advanced strategies, including step-up authentication tailored to specific risk factors. Behavioral biometrics, which analyze user behavior patterns to verify identity, are leading this shift. This approach not only enhances security but also helps firms maintain a smooth customer experience while minimizing friction during the authentication process.

To tackle modern fraud challenges effectively, firms are making significant investments in advanced identity verification tools and synthetic ID detection systems. In fact, **43%** of respondents are directing resources toward imposter detection and identity theft tools, allowing them to stay one step ahead of fraudsters.

Balancing security and user experience

As WAM firms adopt a more proactive stance on fraud prevention, balancing user experience with security has become a top priority. To address this, **57%** of respondents have implemented orchestration platforms that adapt customer friction based on real-time risk monitoring. This industry-leading practice allows firms to halt transactions in real time and conduct manual reviews when red flags are detected, all while keeping customer friction low. Maintaining this balance is essential for safeguarding customers from losses while fostering a user experience that encourages retention.

The growing role of AI in fraud detection and prevention

WAM institutions are actively running proofs of concept to identify the most effective applications of AI within their fraud teams. The goal is straightforward: maximize ROI while leveraging technology to streamline operations and administrative tasks, such as generating case summaries and enhancing transactional and behavioral risk assessments. Currently, **43%** of firms have implemented AI to refine their fraud detection models, while **29%** use it for behavioral analytics. Additionally, **14%** focus on identity verification and **33%** prioritize risk assessment.

This shift toward automation is making fraud prevention organizations leaner and more efficient, allowing them to focus on detection and prevention rather than merely reacting to incidents. Additionally, industry leaders are adopting long-term strategies that harness AI for more impactful purposes, including advanced behavioral and transactional risk assessments, agentic claims investigations and machine learning techniques to identify trends in large datasets.

As firms experiment with GenAI, nearly half of the respondents are exploring its potential for monitoring and incident analysis. However, widespread deployment remains limited due to governance concerns. Many organizations are opting for in-house models or vendor solutions, focusing on automation and regular model updates to minimize errors and enhance efficiency. Specialized vendor tools are also being adopted to address specific fraud types, including check, ACH and wire fraud.

Digital assets and cryptocurrency

Respondents display a cautious approach to digital assets and cryptocurrency, with **100%** reporting a low-risk appetite and are avoiding direct cryptocurrency transactions. Exposure is primarily limited to ETFs or managed funds **(71%)**. Some firms are beginning to monitor wallets and evaluate payments to digital asset firms to identify potential scams.

As firms consider introducing crypto-related products, they are prioritizing upgrades to their existing controls and the development of new ones. This focus underscores the necessity for robust risk management frameworks capable of addressing the unique challenges and regulatory demands associated with digital assets. By enhancing their controls, firms aim to navigate the complexities of the crypto landscape while fostering compliance and safeguarding their operations.

Strengthening defenses through red teaming

In today's landscape, red teaming has emerged as a vital strategy for firms aiming to enhance their fraud prevention efforts. This proactive approach allows an organization to simulate real-world threats to assess control effectiveness and is a leading practice for firms looking to bolster their fraud mitigation strategies. By recreating specific scenarios, either through tabletop exercises or live fire testing, this proactive method allows organizations to identify weaknesses and assess vulnerabilities before fraudsters can exploit them.

However, despite the clear benefits of red teaming, a surprising **67%** of respondents have yet to engage in formal fraud-focused exercises. Many still rely on alternative methods such as tabletop exercises, vulnerability testing and scenario analysis. While these approaches can be beneficial, they often tackle fraud indirectly, focusing more on broader cyber or sanctions-related testing. Some firms express interest in adopting fraud-specific red teaming but cite challenges like coordination complexity and a perceived lack of urgency based on historical loss data.

Yet, the measurable benefits of red teaming are hard to ignore. These exercises can lead to reduced fraud losses, improved regulatory alignment and enhanced customer trust. Firms that depend solely on tabletop exercises or cyber-led red teaming may overlook critical fraud-specific vulnerabilities, particularly in customer-facing processes and nontechnical functions.

To truly bolster their defenses, organizations should move beyond theoretical exercises and embrace intelligence-driven fraud red teaming. This approach validates control effectiveness, identifies gaps and prepares firms for emerging threats. Those already engaged in fraud red teaming set a strong precedent by integrating fraud into their broader risk management programs and continuously updating scenarios based on the latest threat intelligence. In doing so, they not only strengthen their defenses but also position themselves as leaders in the fight against fraud.

8 Organizational strategies for fraud prevention

Internal structures and governance

In the fight against fraud, the internal structures and governance that WAM firms have in place play a crucial role. How these organizations align their fraud prevention efforts can significantly impact their ability to identify and mitigate risks. Recent insights reveal that over half of the respondents position their fraud prevention organizations within the technology and risk groups **(55%)**, while others align them with compliance **(34%)** or cybersecurity **(11%)**.

Establishing a fraud prevention organization isn't a one-size-fits-all endeavor; each approach offers distinct advantages. By aligning fraud prevention with a firm's risk management function, organizations can enhance their overall risk assessment and resource allocation. This integration fosters a comprehensive strategy for identifying and mitigating diverse risks.

When fraud prevention is integrated with compliance, it not only promotes adherence to regulatory mandates but also streamlines reporting and investigations, cultivating a culture of accountability. Additionally, aligning with cybersecurity creates a cohesive strategy to tackle interconnected threats, bolstering data protection and incident response capabilities.

These strategic alignments not only fortify defenses against financial crimes but also drive operational efficiency and regulatory compliance, ultimately protecting both assets and reputation. Regardless of the organizational structure, it is crucial for firms to coordinate fraud management and detection efforts with all stakeholders involved in executing the company's fraud prevention and operational efficiency strategies.

An overwhelming majority of respondents **(85%)** manage identity and authentication under the CISO or the broader cybersecurity function. In this structure, fraud teams often take ownership of fraud detection and prevention processes, while cybersecurity professionals manage the technology and controls necessary for secure authentication. This close collaboration underscores the critical role of cybersecurity in safeguarding sensitive information and preventing fraud.

Breaking down silos for improved collaboration

Respondents have pinpointed significant challenges in fraud risk governance, particularly the silos that hinder collaboration between departments involved in fraud management. In response, firms are prioritizing the integration of fraud risk management across their organizations. By adopting a more coordinated approach, these firms aim to enhance communication and collaboration, allowing for a comprehensive understanding of fraud risks and more effective vulnerability assessments. This shift not only streamlines processes but also fortifies defenses against evolving threats.

A notable trend emerging in the industry is the establishment of fraud fusion centers, which align operations, such as fraud prevention and AML, to create efficiencies and foster a more holistic understanding of the financial crimes affecting business. Currently, **33%** of WAM firms have successfully integrated their fraud and AML functions. However, the majority **(67%)** do not plan to change their formal organizational structures. Instead, they are focusing on increasing collaboration among fraud, AML and cybersecurity teams, underscoring the critical need for cohesive strategies to tackle complex financial crimes effectively.

Adaptation and continuous improvement

Adapting to the evolving fraud landscape requires a proactive and comprehensive approach. As fraudsters become more sophisticated, WAM firms need to stay one step ahead by implementing proactive measures that not only address current threats but also anticipate future challenges. However, while technology and collaboration are vital, the human element remains a key line of defense. Ongoing training and awareness programs for staff are essential to equip employees with the knowledge they need to recognize and respond to potential fraud.

9 Contact us

To learn more about our fraud and broader financial crime prevention offerings, please reach out to any of the team members on this page or your usual EY US contact.

Walid Raad
US Forensics Financial Services Leader
Ernst & Young LLP
+1 212 773 0956
walid.raad@ey.com

Arpi Lal
Partner
Ernst & Young LLP
+1 212 773 3038
arpi.lal@ey.com

Robert Mara
Principal
Ernst & Young LLP
+1 212 773 1025
robert.mara@ey.com

Clay Roberts
Senior Manager
Ernst & Young LLP
+1 212 773 9481
clay.roberts@ey.com

Bob Boyle
Managing Director
Ernst & Young LLP
+1 212 773 1335
bob.boyle@ey.com

Nick Spinella
Senior Manager
Ernst & Young LLP
+1 212 773 6357
nicholas.spinella@ey.com

EY | Building a better working world

EY is building a better working world by creating new value for clients, people, society and the planet, while building trust in capital markets.

Enabled by data, AI and advanced technology, EY teams help clients shape the future with confidence and develop answers for the most pressing issues of today and tomorrow.

EY teams work across a full spectrum of services in assurance, consulting, tax, strategy and transactions. Fueled by sector insights, a globally connected, multi-disciplinary network and diverse ecosystem partners, EY teams can provide services in more than 150 countries and territories.

All in to shape the future with confidence.

US SCORE no. 29991-261US_2

2508-10704-CS
ED None

ey.com