Wealth and Asset Management

Fraud Insights Point of View

Results and insights

Second edition – May 2024

Building a better working world

Background

Ernst & Young LLP (EY US) issued the first edition of the ***Wealth and Asset Management Fraud Insights Point of View*** in 2022, providing an in-depth analysis of the fraud landscape and how wealth and asset management (WAM) institutions are addressing the unique challenges around fraud. This second edition of the WAM Fraud Insights Point of View (POV) will enrich prior findings based on fresh perspectives and comparisons, giving insights about market shifts and future fraud strategies for financial institutions. The EY US team engaged in discussions with both new and previous respondents, each with retail operations and assets under management ranging from $1 trillion to $10 trillion.

Because of the availability of data, not all respondents could answer every question. The percentages in this POV will be 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).

Key themes identified

- **Respondents continue to cite technology as a top priority for the firm**. Many respondents indicated that maintaining and continually enhancing their existing technology stack to stay ahead of fraudsters' tactics was a primary challenge for the organization. As technology continues to advance and new capabilities emerge, the existing tools and platforms are becoming outdated more quickly, forcing firms to more frequently re-evaluate their current infrastructure.

- **Artificial intelligence (AI) is a top-of-mind issue for firms throughout the industry**. Respondents are exploring how their fraud teams can capitalize on the technology to better prevent and detect fraud and make the investigation process more efficient. Meanwhile, firms also must prepare for the threat of bad actors exploiting AI to perpetuate fraud against firms and their customers. Firms are working to understand both sides of this capability and what it means for the future of fraud.

- **Financial exploitation was a renewed area of focus this year, as fraudulent activity targeting vulnerable investors, particularly elderly customers, has increased over the past year**. Firms are proactively looking to industry to assess liability and determine leading practices to help protect their vulnerable customers and prevent financial and reputational harm.

- **Respondents are continually evaluating their current structure and where the fraud organization should sit within the overall institution**. Agnostic of whether the fraud organization sits in the first or second line of defense, there is a varying degree of involvement of the fraud organization in key functions such as risk management, customer onboarding and insider threat.

- **The reporting structure, roles and responsibilities of insider threat programs continue to vary throughout the industry**. The majority of respondents use a hybrid model with multiple teams and involve their legal team when investigating and responding to insider risk events. While some respondents were leveraging automated channels for reporting, most respondents rely on manual reporting functions as the primary intake for insider risk incidents.

- **Respondents reported that scams reflected the largest uptick in fraud exposure experienced over the last year**. Firms saw an increase in cases and losses attributable to customer scams and are currently evaluating how they are going to track and handle scams going forward. While some firms have started proactively tracking detailed scam metrics, most respondents are not currently tracking metrics for specific scam typologies.

- **Overall, the respondents have experienced an increase in loss per successful fraud incident year over year**. While firms continue to bolster their existing control framework, resulting in less successful fraud incidents, the overall loss per incident has increased.

- **Respondents use different measures to quantify fraud losses, which can be defined by either customer or firm losses**. It is important that firms clearly determine the way they want to define specific fraud and scam typologies to consistently calculate fraud losses and properly quantify the level of fraud risk exposure.

- **Respondents have differing methodologies for calculating prevented loss**. Some respondents include proxy amounts or include assets at risk in their calculations, while other firms only include transactional avoidance.

The future of fraud

EY US point of view

Based on our conversations with WAM firms and the current market trends observed, we suggest that firms take into consideration the following leading practices to proactively address fraud trends and be better prepared to succeed in the evolving fraud landscape.

Firms should seek to enhance their fraud tracking capabilities pertaining to fraud typologies, specifically scams. By clearly tracking and categorizing different fraud and scam typologies, firms can take a more data-driven approach when tailoring their control framework. As firms work to improve their tracking and reporting capabilities, they will have opportunities to better define and understand their unique fraud exposure and related losses. This will be critical as firms work to better understand the vulnerabilities that are leading to firm and customer losses.

Firms will need to apply more friction (e.g., slowing down instant payments with a high risk score) to the customer experience and emphasize education for existing customers and employees as key enhancements to their preventative control framework. Given the complex nature and sophistication of recent scams observed, customers are being coerced into authorizing fraudulent payments out of their account more often than in previous years. Education about relevant fraud typologies and the ability to slow down the movement of funds when red flags are identified are going to be essential to mitigating fraudulent activity before it takes place. Firms must work to understand how much intervention they should add to the money movement and onboarding process to fight scams and fraudulent account openings.

Firms must be diligent and consistent in their assessment of their own liability when a successful fraud event occurs. Most firms typically reimburse customers when there is a breakdown in the firm's control framework. In addition to a sound preventative framework, firms should establish clear procedures to effectively identify customer-initiated money movement resulting from fraud and come to a consistent remediation decision. In doing so, firms will have taken into consideration the threat of litigation, regulatory action and reputational harm when making the decision to reimburse their customers.

Firms should continue to prioritize the implementation of AI and machine learning as it becomes more commonplace throughout the industry. The need for effective AI tools will be driven by increasingly sophisticated fraudsters who are leveraging the same AI technology to find new vulnerabilities and continue to find ways to breach firms' control frameworks. Firms will need to determine how to best implement this new technology while staying current on the newest methods being leveraged against them. Capabilities that were considered cutting-edge from last year, such as voice biometrics, have already been proven to be vulnerable to more advanced techniques used by fraudsters, and firms will have to keep this threat in mind when evaluating their current risk and control framework.

Key takeaways

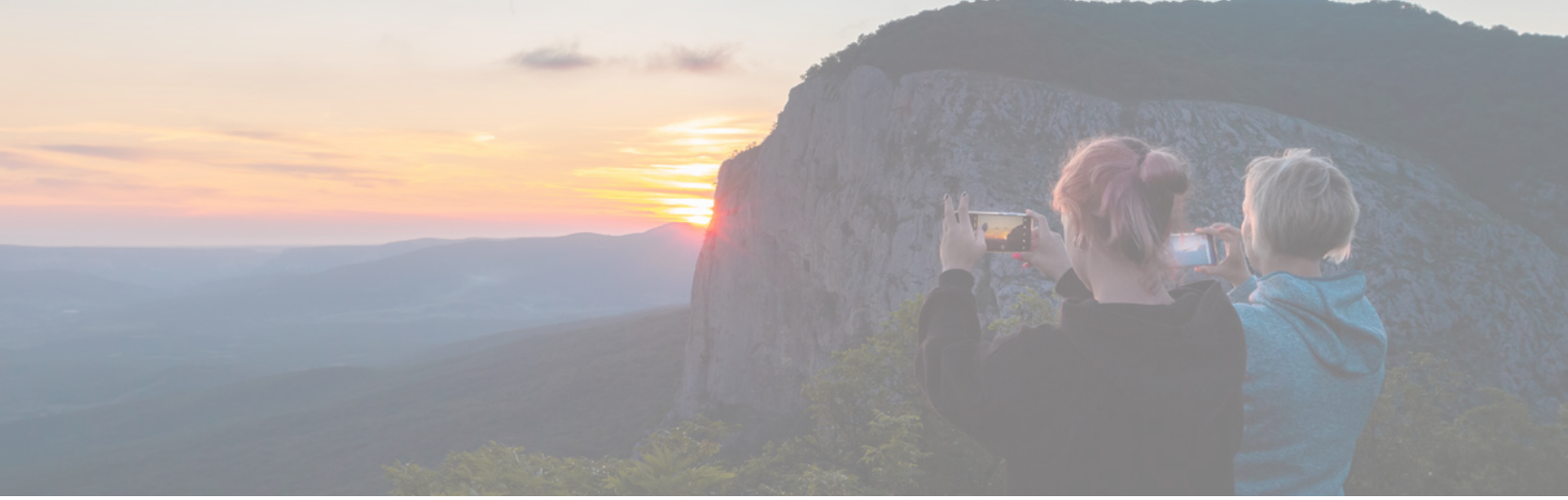
As the tactics and technology used by fraudsters become increasingly sophisticated and scams continue to emerge and outpace regulatory liability guidance, firms and their customers are looking for the best ways to defend themselves against these complex schemes. It will become increasingly important that firms enhance the way they are addressing and tracking scams. This will include updating their control suite with the most current technology, such as AI and machine learning, and using their reporting metrics to equip the institution with powerful insights that will be leveraged to enhance their risk management framework. When fraud occurs, the distinction between customer loss and firm loss will continue to be a focal point for firms and regulators. Determining whether the fraud occurred as a result of customer action or a breakdown in controls will become increasingly important to assess liability as fraud schemes and scams continue to evolve. Customer loss has the potential to lead to firm loss, an increase in litigation, potential regulatory action and reputational harm. **In our discussion with respondents, we observed that up to 30% of customers leave an organization after falling victim to a scam, regardless of whether the loss was due to a breakdown of controls or initiated by the customer**. Firms must continue to improve and evaluate their fraud program and customer education to better defend themselves and their customers from these ongoing risks.

1

Top challenges

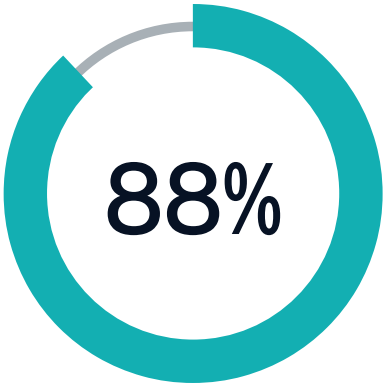
There was consistency among respondents regarding the top three challenges facing fraud organizations. **The most common challenge highlighted by 88% of the respondents was updating their technology stack to address vulnerabilities and enhance the preventative control environment**. As fraud is constantly evolving and new threats are emerging (e.g., AI impersonation scams), firms are constantly trying to keep their fraud infrastructure and technology up to date.

Many respondents indicated that they were evaluating their current technology stack to determine if controls were up to date and performing as expected. **More than half of the responses received indicated that firms made technology investments that did not perform as well as expected**. Underperforming investments included their case management tools, fraud detection methods and analytical tools, with some respondents also expressing that their existing tools have simply become obsolete and are struggling to keep up with the advancement in fraud tactics. **Some respondents reported that certain channels and tools were resulting in false positive rates up to 99%, leading to a high volume of reviews and inefficiencies in the alert review process**. Voice biometrics is another tool firms indicated was not meeting expectations, as they are experiencing difficulty with user adoption and fraudsters have already leveraged AI to perform voice re-creation, decreasing the utility of the control.

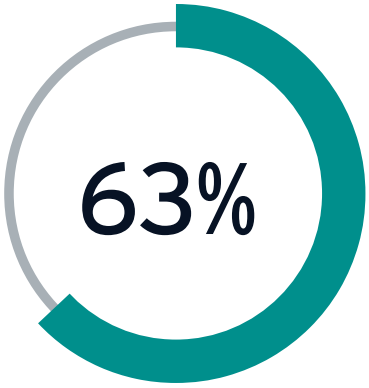


Most of the respondents (63%) noted challenges surrounding their firm's staffing and operational structure. Many firms are re-evaluating the structure of their fraud organization and where certain responsibilities sit, such as the role the fraud investigation unit plays during customer onboarding, who should be involved to address internal threats and insider risk, and how integrated the anti-money laundering (AML) and fraud organizations should be. Firms are looking for more effective ways to retain their key resources and keep them current on the evolving fraud landscape while building the cohesiveness and efficiency of their business units, sometimes having to consider coordination across international teams.

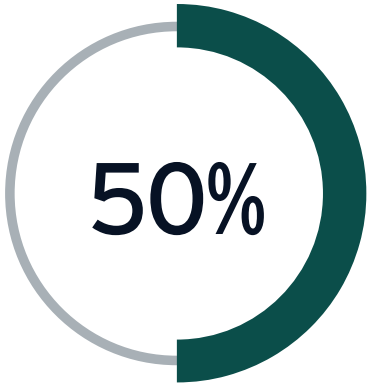
Half (50%) of the respondents are working to manage increased fraud volumes. Some respondents saw as much as 10 times the amount of fraud over the past three years. This increase in fraud strains the existing fraud infrastructure and organization. Firms are exploring ways to leverage AI and other analytical tools to help screen transactions and detect fraud. Additionally, firms are looking for new ways to respond and help prevent their customers from falling victim to scams. Industry leaders are looking to employees from across the business (e.g., call center employees, investment advisors) to help in the fight against scams and to help determine the true intention behind transactions. By detecting red flags early and educating customers, firms are hoping that they can help prevent scams before they take place.



of the respondents are updating their technology stack to address vulnerabilities.



of respondents noted challenges surrounding their firm's staffing and operational structure.



of respondents are working to manage increased fraud volumes.

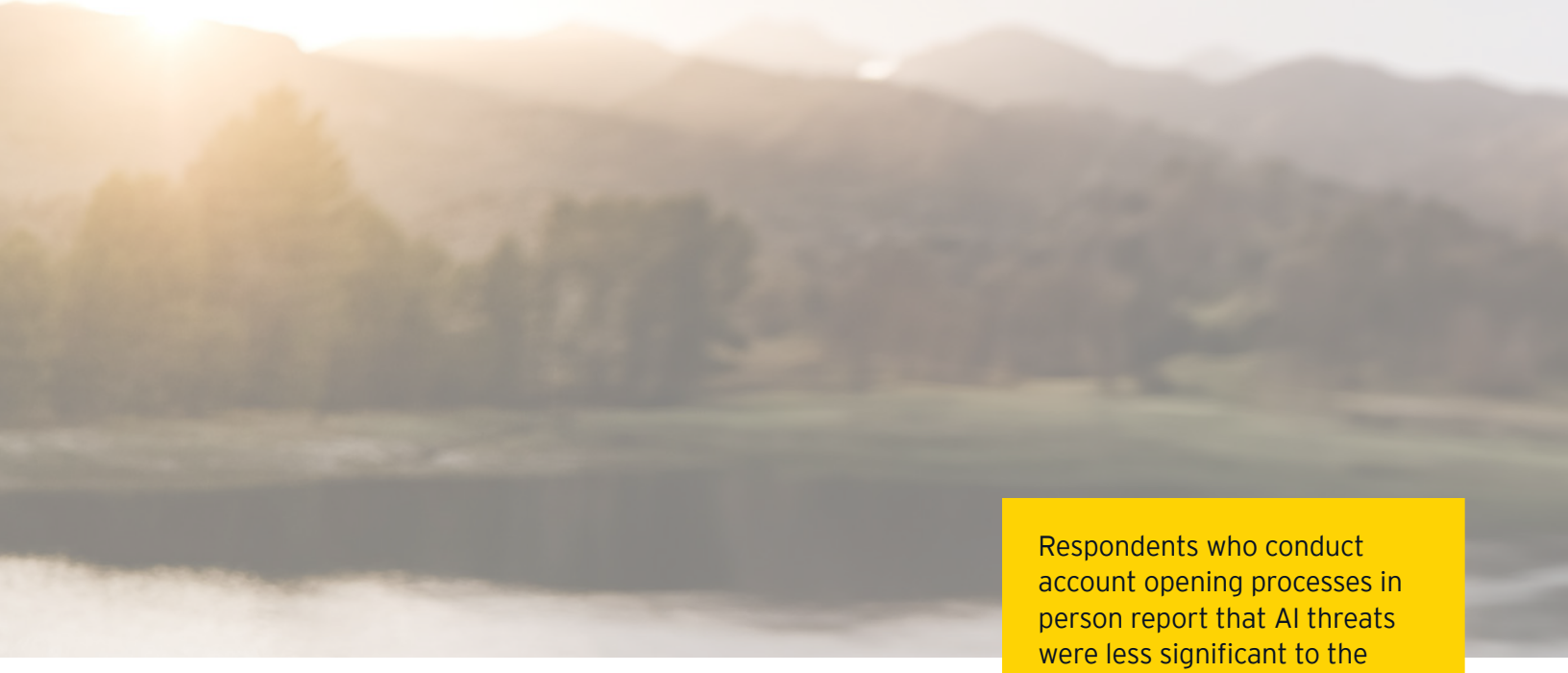
2 Strategic initiatives

All respondents consider technology as at least one of their strategic initiatives in the coming year. **Respondents continue to report that preventative technologies were top of mind and many firms have shifted focus to AI integration**. Firms are trying to determine how AI and machine learning can help with data mining, detection of abnormal behavior and improving investigation efficiency.

Other strategic initiatives span the broader fraud risk management framework and include enhancing analytics and reporting metrics, further refining the staffing model, improving review efficiencies and enhancing authentication practices. A challenge that many respondents are facing in working toward these strategic initiatives is around budget restrictions.

3 The impact of AI

AI is top of mind at every institution. Firms are both preparing to defend against fraud threats presented by AI and exploring the use of the technology to help prevent and detect fraudulent activity. Discussions with the respondents revealed that firms are at different stages in their approach to adopting AI. Three-quarters (75%) of the respondents indicated that they were currently leveraging AI, working to identify the appropriate applications for their business or further developing their current AI capabilities. Industry leaders have implemented AI to improve scam detection and investigation efficiency, reduce false positives on fraud alerts, reduce operational cost and aid in the suspicious activity report (SAR) filing process.



Respondents who conduct account opening processes in person report that AI threats were less significant to the organization. These firms find that leveraging their investment advisors and in-person relationships provide substantial barriers to would-be fraudsters.

Some (43%) of the respondents are already taking measures to prepare for external AI risks. These firms specifically highlighted the risk of overriding controls, such as bypassing voice biometrics, or impersonating firm employees during customer outreach as being some of the top threats associated with AI. Firms are looking to upgrade their controls and provide additional education to their internal resources to prepare for this upcoming threat. It is worth noting that the respondents who did not allow online account opening did not consider the threat of AI as pressing as those who did allow online account creation. These firms are finding that because they are leveraging their investment advisors, the in-person relationship components of the process are providing substantial barriers to would-be fraudsters.

4 Combating specific types of fraud

Bot attacks continue to be an area of high risk, according to the respondents, because an identified vulnerability can quickly lead to high volumes of attempted fraud driven by the automated nature of these attacks. Of the impacted respondents, **100% of participants are using some form of fraud detection and rule-based alerting to specifically identify bot-related typologies**. Being able to perform behavioral analytics at account opening is a key tool in identifying these attacks and shutting down the related accounts before any money movement can occur.

Synthetic ID fraud continues to be another area of focus. Of the impacted respondents, **60% rely on external vendors to identify the specific typologies related to the fake or compromised personally identifiable information (PII)**, while 40% of the responses show that firms are simply leveraging their typical know your customer (KYC) and customer identification program (CIP) processes to identify manufactured profiles.

5

Leading fraud concerns

In our discussions with respondents, the top three fraud risks identified were account takeover (ATO), scams and new account fraud (NAF). ATO represented 88% of respondents, while scams and NAF represented 63% and 50% of respondents, respectively. Some prevalent fraud risks related to the top three fraud concerns include automated customer account transfer (ACAT), counterfeit checks, compromised credentials and social engineering. Respondents noted that ACAT fraud is particularly troublesome, as it typically involves high dollar transfers between different institutions, limiting transparency on either end of the transactions.

Top three fraud risks

This year, 75% of the respondents stated that the most significant increases in fraud observed were related to scams. This trend presents a shift from prior market studies in which the increases in fraud were predominantly driven by ATO and NAF. **About two-thirds (67%) of this year's respondents who noted the large increase in scams' volume also noted that they were observing the most change in fraud typologies with new scam trends**. Scams pose a unique challenge because of their high frequency compounded by their potential to cause significant financial losses, mostly to customers. Respondents reported that the most prevalent scams experienced this year were specifically impersonation scams, romance scams and business email compromise.

According to the Federal Bureau of Investigation (FBI) 2023 Internet Crime Report, the customer scams with the highest losses were:

$4,570.3 million Investment scams	$2,946.8 million Business email compromise	$1,278.6 million Data breach
$924.5 million Tech support impersonation	$652.5 million Confidence/romance scams	$394 million Government impersonation

Source: FBI 2023 Internet Crime Report

Most common fraud categories in 2023, according to the Federal Trade Commission (FTC) Consumer Sentinel Network

Imposter scams	Online shopping and negative reviews	Prizes, sweepstakes and lotteries	Investment scams
33% Percent of fraud reports	14% Percent of fraud reports	6% Percent of fraud reports	4% Percent of fraud reports
$2,668.1m Customer losses ($)	$392.2m Customer losses ($)	$337.9m Customer losses ($)	$4,641.9m Customer losses ($)
27% Customer losses (%)	4% Customer losses (%)	3% Customer losses (%)	46% Customer losses (%)

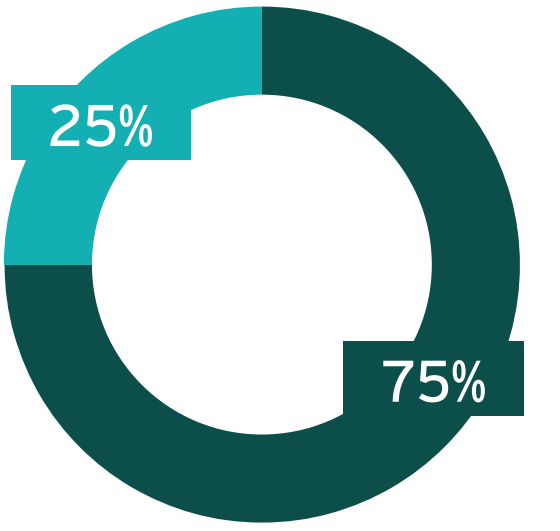
Source: FTC Consumer Sentinel Network Annual Data Book 2023

6

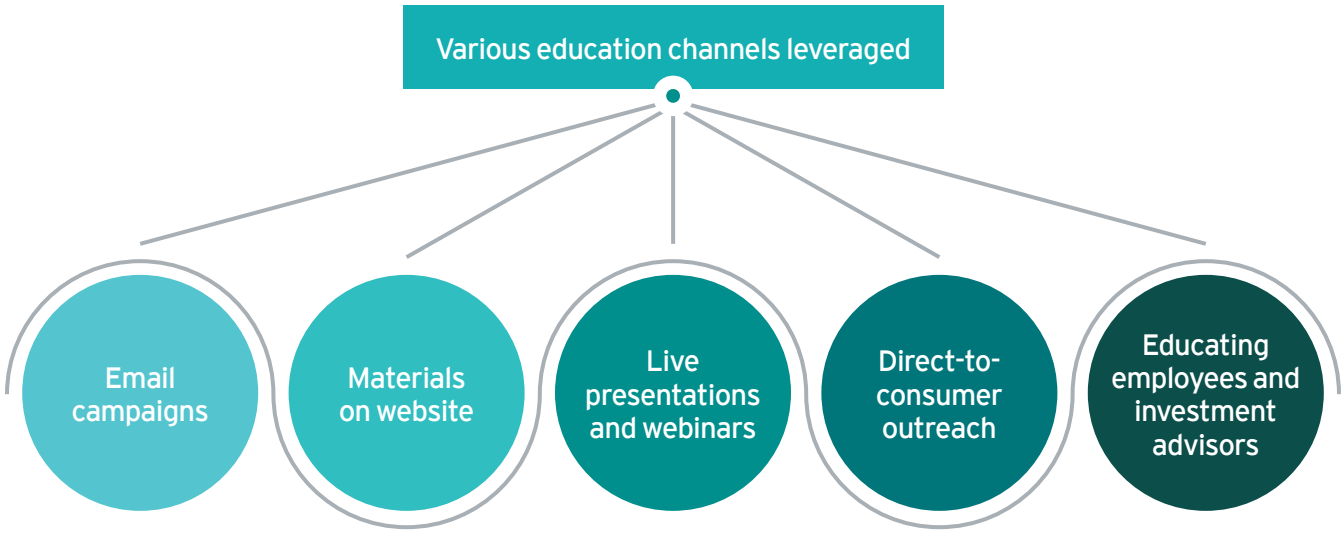
Scams

As scams have seen the highest increase in activity over the past year, tracking scams has also become a focus of fraud organizations across the industry. **Industry-leading firms are leveraging insights gained from tracking specific types of scams to drive preventative measures such as control enhancements (e.g., introducing customer friction into money movements) and tailored educational updates for investment advisors and customers.** Some respondents have already enhanced their reporting to define scams by typologies and track their specific occurrences; however, most respondents indicated that they were not differentiating or categorizing by scam type. Typically, firms are identifying fraud that occurred and classifying these instances under a single umbrella, rather than separating them by individual typologies (e.g., impersonation/imposter, romance, investment). By clearly tracking and categorizing different scam typologies, firms can better address specific threats that are impacting the business and their customers.

Firms tracking specific scam typologies



Customer education is a key tool in preventing fraud resulting from scams. All respondents have indicated that they are providing customer education regarding scams through various channels, including updates on their websites, live presentations/webinars, notifications through firm apps and direct-to-consumer outreach (e.g., email campaigns). **Additionally, 63% of the respondents indicated that they were providing continuous education around scams to employees and investment advisors**. Education and training specific to the common scams impacting the organization will better equip customers and employees to identify the red flags and prevent fraudulent activity resulting from scams.



"

The most crucial step to avoid being scammed is knowing what could happen and discussing it with family and friends. When people are aware of a specific scam, they are 80% less likely to engage with it, and if they do engage, are 40% less likely to lose money or sensitive information.

Source: CNBC, based on data from the Financial Industry Regulatory Authority (FINRA)

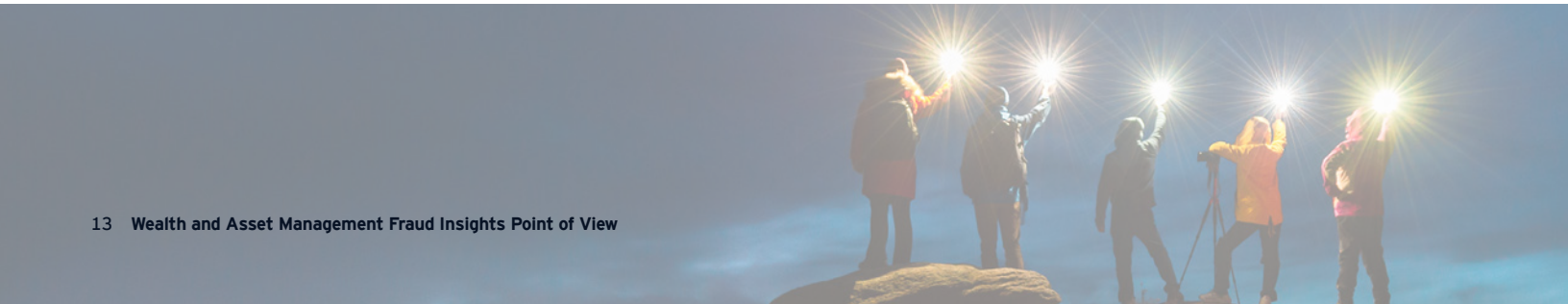
7

Firm losses

There is a growing initiative across the respondents to begin differentiating data for various types of fraud observed, specifically with a focus on fraud originating from scams; however, only 25% of the respondents have already enhanced their reporting to track loss metrics surrounding specific fraud typologies. It is increasingly important for firms to track fraud data granularly to develop a more data-driven and proactive approach in responding to fraud. By tracking metrics tied to specific fraud typologies, respondents indicated that they are more informed on the current risks and better equipped to bolster their risk management framework and develop proactive fraud prevention strategies. The firms that leverage a data-driven approach have positioned themselves to identify patterns, trends and anomalies. This insight can be leveraged to better assess and manage risk exposure and help implement risk management policies and controls for the early detection and prevention of fraudulent activity and scams. Additionally, firms can leverage the insights gained from tracking these metrics to better understand the specific scams targeting their customers. This allows them to provide more personalized guidance to customers to better protect them against fraud. Conversely, the majority of respondents that do not granularly track fraud typologies run the risk of misallocating resources to less significant issues and pulling resources away from their largest areas of exposure. Customers' knowledge that their financial institution is actively monitoring and working to prevent fraud can significantly increase trust and confidence in the institution and help firms protect their brand and reputation.

For the responses received, participants experienced an average of approximately 370 successful fraud incidents resulting in about **$250,000 to $22 million in losses to the firm**. The average net firm loss per fraud event ranged from approximately **$11,000 to $185,000 per successful fraud incident**. Respondents experienced over **2,000 successful firm loss incidents**. Most firms saw an increase in annual realized fraud losses between FY22 and FY23, with some experiencing over a **250% increase**.

The increase in scams can be attributed to several key drivers. Digitalization has made online financial transactions more accessible, providing fraudsters with more opportunities to exploit digital system vulnerabilities. Simultaneously, scammers have grown more sophisticated, leveraging AI and social engineering techniques to deceive customers and financial institutions. The situation is exacerbated by large-scale data breaches, which expose sensitive information, paving the way for fraudsters to impersonate both customers and employees successfully. There has historically been a lack of awareness about scams among consumers and employees, which contributes to their susceptibility to exploitation. This is particularly true for the elderly demographic, who typically are less familiar with these scams and therefore more prone to fall for them. Finally, the globalization of the financial system has enabled fraudsters to execute their operations across borders, complicating law enforcement's efforts in tracking and prosecuting them. **As a result, control frameworks often struggle to keep up with evolving scam tactics, thereby inadvertently creating loopholes for scammers to exploit**. To address these challenges, industry-leading firms have been successful in maintaining their level of fraud losses by implementing a bolstered control framework (e.g., enhancing authentication measures and leveraging device metrics), enhanced procedures surrounding detection and due diligence, and increased education around new fraud trends and scams.



8

Prevented loss

While realized fraud losses are an important data point for fraud risk management, it is also important to understand prevented losses to assess effective control designs and preventative measures that can be leveraged to further enhance the control framework. Prevented losses are calculated differently among the respondent firms; however, overall, the term refers to the potential loss that was avoided because of preventative control measures that stop fraud before it occurs. Prevented loss calculations can include the total dollar amount of fraudulent transactions attempted, as well as fraudulent deposits made into the organization that are not sufficiently funded and blocked before the funds can leave the account. Half of the respondents reported that they leverage the transactional approach to calculate prevented loss. The transactional approach to calculating prevented loss encompasses transactions and attempts at moving money but do not include soft avoidances and instances where an account has been compromised and/or unauthorized access has been gained. The remaining respondents include fraudulent accounts opened with no money movement or attempted fraudulent access (e.g., fraudulent login attempts), including the total relationship value or assets at risk in the prevented loss calculation.

Leveraging the transactional approach for calculating prevented losses, the total prevented loss for respondents was $1.325 billion in 2023. It is worth noting that the total prevented loss can vary greatly depending on whether factors beyond those directly associated with money movement are incorporated into the calculation.

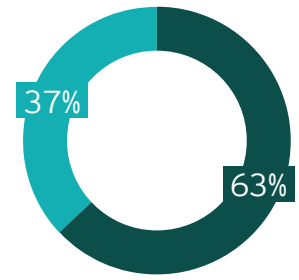
Respondent firms averaged

$221 million

in prevented losses in 2023

When financial loss occurs, asset recovery is typically handled by the fraud investigation unit identifying the fraudulent activity. When the investigations unit is not driving the recovery efforts, they facilitate asset recovery by coordinating with the firm's front-line units, which can include product-specific teams, such as wire and check teams.

Teams responsible for asset recovery



Effective, real-time communication across first and second line operational units is a leading practice for organizations seeking to recover fraud loss. Conversely, isolated teams that are not aligned can experience limitations in their recovery efforts. If the fraud unit is solely responsible for recovery efforts, it is important to balance recovery tasks with their primary investigation role. Operational units can provide significant support, leveraging key customer data and process knowledge to help with efficient fund recovery. This coordination between fraud investigation units and operational units can impact how effective firms are at recovering funds quickly and can potentially help keep investigations uninterrupted for the asset recovery process.

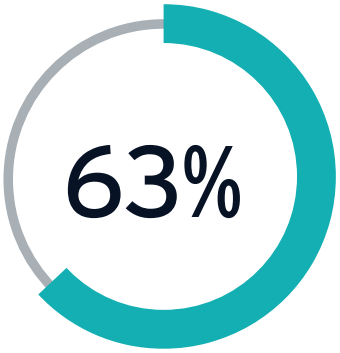
9

Organizational structure

Most of the respondents align their fraud organization to the second line of defense, while the remaining respondents align it to their first line of defense. Aligning the fraud organization with the first line of defense can provide its own benefits, like more efficient communication with the front office. Their insight into daily operations can also aid in spotting vulnerabilities and opportunities to refine the controls framework, such as the need for additional employee training. Conversely, aligning the fraud organization with the second line of defense can lead to a more focused effort on fraud detection or on providing an outsider's perspective when assessing potential operational vulnerabilities. Regardless of where the fraud organization sits within the firm, **it is imperative that it coordinates fraud management and detection functions with other stakeholders who can execute company strategy and procedures for fraud prevention, detection and operational efficiency**.

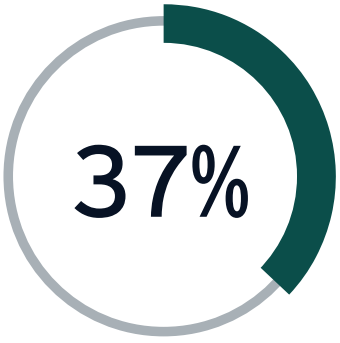
Most respondents reported that their fraud organization sits within the risk or compliance groups with some firms choosing to position the fraud organization under the chief information security officer, aligning cybersecurity and fraud prevention. Other respondents noted that their fraud organization aligns with their financial crimes unit, which can help with communication and coordination between the organizations.

Where the fraud organization is positioned in the firm



2nd line of defense

VS.



1st line of defense

10

SAR filings

An overwhelming majority (88%) of respondents maintain separate organizations for fraud and AML, though they often work closely together. For 12% of the respondents, AML and fraud operations are combined.

For the respondents where the AML and fraud organizations are integrated, the combined unit is responsible for filing all AML- and fraud-related SARs. For the firms where the AML and fraud units are separate, fraud SAR filing responsibilities are shared by the fraud, financial crime and AML teams.

While fraud and AML are generally separate functions within the respondents' organizations, there can be a significant level of overlap in the tools leveraged and resources available. To facilitate effective communication, the organizations must share trends observed, best practices and effective monitoring capabilities to allow for a comprehensive financial crime prevention framework.

Fraud SAR filing responsibilities

11

Operational capacity

The size of the external fraud organization varies significantly across different respondents, ranging from as few as six people in the investigation unit to as many as 200 people globally. Additionally, half of the respondents use external vendors, contractors or managed services to support their fraud organization.

In 2023, respondents experienced a downtick in coordinated attacks that resulted in huge volumes of NAF and ATO. This can be attributed to an emphasis on bolstering the preventative control framework, such as the implementation of machine learning models, as well as on enhancing processes that reduce vulnerabilities to such events and accelerated detection when a pattern is apparent.

When large-scale fraud events (LSE) occur, 57% of the respondents form ad hoc teams to focus on the influx of volume and handle the risk specific to the patterns being observed. To help with the increase in volume, firms have implemented efficiencies through efforts like developing playbooks to expedite the response time to an LSE and making sure processes are already established, including outreach to all relevant stakeholders, such as members from management, AML, KYC, compliance and legal teams.

12

Customer onboarding

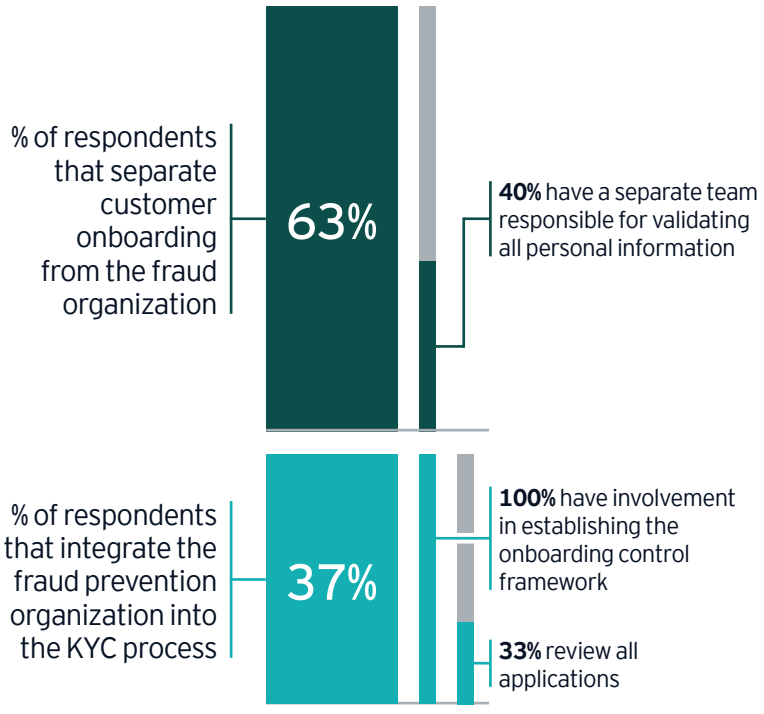
Most of the respondents separate customer onboarding from the fraud organization. The segmentation of roles necessitates strong communication to assist in efficient coordination and to make sure there is adequate fraud oversight in the account opening process. Some respondents noted that they involve a specialized team responsible for validating all personal information provided or conducting its enhanced due diligence process when red flags are identified. Some fraud organizations are even further integrated into the onboarding process, with involvement in the establishment of the rule-based alerting process leveraged.

Reflected in results illustrated below, 37% of respondents stated they have the fraud organization integrated into the KYC process and review applications before accounts are opened. As part of this integration, all respondents are thoroughly involved in establishing the onboarding control framework (e.g., customer risk rating methodology) the onboarding team leverages, with some responsible for reviewing every application that comes through. While this approach introduces more friction during onboarding, the fraud organization gets involved at the earliest stages of the relationship and can help mitigate fraud risk by detecting potential fraud risks sooner, shifting from reactive management to proactive prevention.

Most respondents stated that their CIP is handled outside of the fraud organization. For the firms that integrate their fraud organization with the customer onboarding process, most respondents indicated that they have either implemented new tools to help with CIP or were in the process of upgrading their platform. Firms have had to adjust their process to identify high-risk populations and perform additional reviews, with some firms completely shutting down certain processes (e.g., check writing) when there was too much exposure.

It is worth noting that **some respondents either limit or do not allow online account opening**, which greatly mitigates the risk of bot attacks and synthetic ID fraud, as much of the account opening process is largely conducted through a relationship manager.

Involvement of fraud organization in customer onboarding at overall level



13

Fraud intake channels

It is important that organizations implement a wide range of tools and strategies to prevent and detect fraudulent activities. **Fraud intake is a key component to identifying potential red flags, allowing companies to be more informed of their fraud exposure and where to implement preventative measures**. As such, participant organizations noted they are leveraging both manual and automated intake channels. Manual intake channels include monitored fraud hotlines, chatbots and manual referrals repositories originating from front-office relationship managers and investment advisors. Cyber teams and customers can also refer cases to the fraud organization following identified fraud red flags. Automated intake methods largely consist of alerting functions that flag suspicious transactions or activities for proactive investigation. Different firms use varying systems of red flag monitoring or reporting that can be triggered by actions like automated clearinghouse (ACH) account/external account authentication and identity theft alerts. It is also common for accounts with traditional banking services (e.g., bill pay, checking) to have alert systems set to notify the fraud organization of any atypical activity.

Three-quarters (75%) of the respondents have a general queue for the referrals that the investigators work through. **While some firms have staff aligned to specific product offerings or fraud detection strategies, most resources are centralized with investigators trained to handle all types of fraud**. While there tends to be no triage process in place for specific kinds of fraud/patterns observed, firms prioritize higher-risk referrals or alerts, resolving cases involving money movement first to minimize or prevent fraud losses.

Fraud intake channels

Manual channels

- Suspicious activity referral form
- Customer reported via phone/email
- Referred from other lines of business (i.e., financial advisor)
- Monitored chatbot

Automated channels

- Identity theft alerts
- Suspicious login alerts
- Suspicious transaction alerts
- External account verification alerts

14

Insider threat

Respondents continue to note varied approaches regarding the responsibility and oversight of the insider threat program and insider risk management. **While 25% of the respondents indicated that their external fraud organization also handles internal fraud investigations, 75% of the respondents indicated that they leverage a separate business unit to review internal fraud.** Of the respondents who leverage a separate business unit, 33% have a dedicated internal investigations unit, while some use a hybrid model with multiple teams across the firm playing a role in the investigation and monitoring of internal threats. The legal and risk teams are often involved, and the responsibility of detection and investigation often sits with audit or global security teams. For the responses provided, some respondents have insider threat detection under the risk organization, while the investigation function sits with the legal team. Whether internal fraud is handled by the external fraud organization, a separate dedicated team or a hybrid model, the involvement of the legal team was common among most respondents. For an insider threat program to be effective, teams must be empowered with the appropriate tools, resources and clear escalation paths. Insider threat teams are more likely to succeed when the process is visible throughout the organization, information is shared appropriately across teams and the separation of roles is defined.

For the responses received, all the respondents are leveraging manual reporting functions (e.g., employee reporting, customer reporting, anonymous hotline functions) as the primary intake for incidents specific to insider risk. **A majority of firms are attempting to move into a more proactive position, with 57% of the respondents building out additional models and monitoring tools to identify suspicious activity and anomalous behavior**. The threat of unauthorized communication channels has been a main focus when building out these proactive tools. With the expansion of remote work in recent years, the risk posed by unauthorized communication channels has significantly increased. Regulators have been focused on the use of off-channel communications by employees, and financial institutions have collectively paid billions in fines. When designing these proactive tools, organizations must consider the potential risks presented by remote work and continually evaluate controls over unauthorized communication channels. Overall, insider risk is an area that continues to be a focus, and firms are continuing to evaluate and improve their current framework.

25%

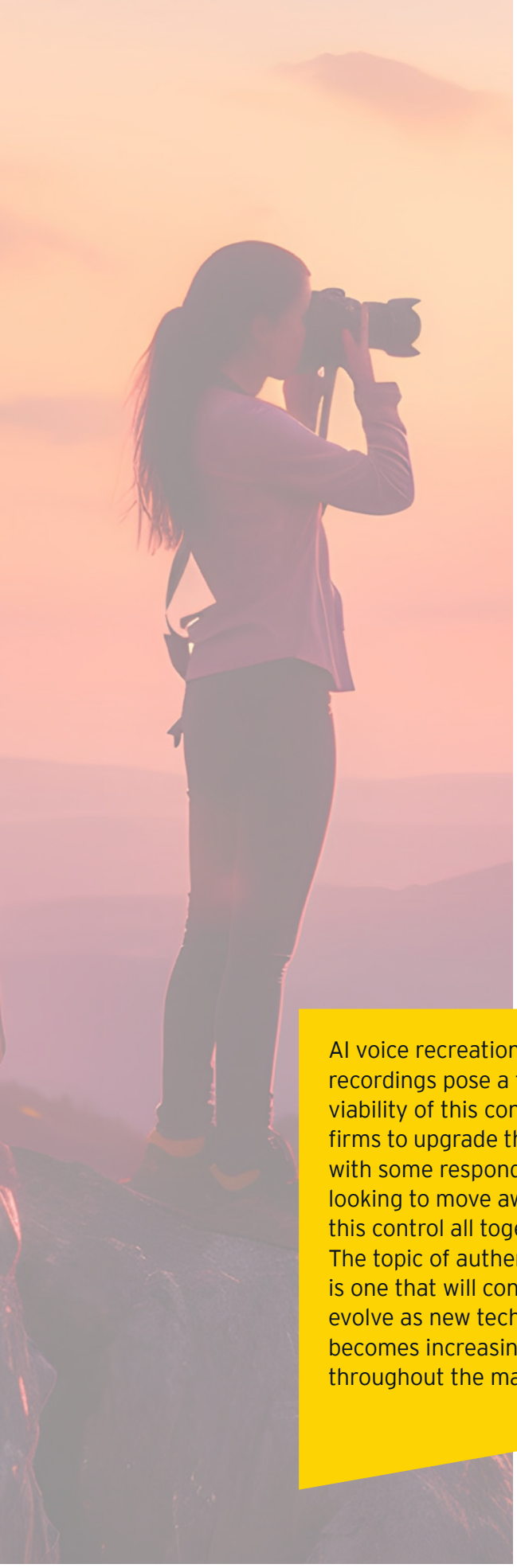
of respondents indicated that their external fraud organization also handles internal fraud investigations.

75%

of respondents indicated that they leverage a separate business unit to review internal fraud.

57%

of respondents build out additional models and monitoring tools to identify suspicious activity and anomalous behavior.



15

Authentication

Over the past few years, there has been an increased focus on leading practices surrounding the customer authentication process. **As PII has become more vulnerable to bad actors and enhanced AI capabilities make it easier to impersonate customers, firms are looking for improved methods to authenticate their customers**. To enhance their existing framework, industry leaders have started to move away from traditional means of authentication, instead incorporating biometric and multifactor models. **Enhancements include increased authentication for higher-risk customers and activity. Firms are even requiring outreach and future communications with the customer when atypical account behavior is identified**. Additional processes leverage face and ID scanning, requiring a government ID and new photo of the customer to compare with records and verify that the person executing transactions is known to the firm.

AI voice recreation and voice recordings pose a threat to the viability of this control forcing firms to upgrade their platform, with some respondents even looking to move away from this control all together. The topic of authentication is one that will continue to evolve as new technology becomes increasingly prevalent throughout the market.

One area of authentication many respondents discussed was voice biometrics. **Half (50%) of the respondents stated that they were leveraging voice biometrics**; however, those same firms expressed difficulty in getting customers to adopt this feature and concerns over the threat of AI and the ability to override this control. AI voice re-creation and voice recordings pose a threat to the viability of this control, forcing firms to upgrade their platform, with some respondents even looking to move away from this control all together. Authentication is one topic that will continue to evolve as new technology becomes increasingly prevalent throughout the market.

16

Financial exploitation and liability

Of the responses received, 100% of the respondents noted an increase in financial exploitation, specifically targeting vulnerable investors. Vulnerable investors can include elders or others who may be more susceptible to financial exploitation because of their age or a cognitive disability. Respondents reported that they are the most susceptible to scams before any preventative controls can take effect. To combat this, industry leaders have implemented enhanced preventative controls to identify potential instances of exploitation, such as implementing security measures that restrict online access when accounts have been inactive for a certain period. **Another industry-leading use case is assessing vulnerable accounts for changes in behavior, such as elderly customers who have increased outreach or online login attempts that are closely followed by large transactions**. Establishing cluster models for elderly customers can also help firms detect deviations from anticipated behavior. Additional monitoring can include triggering alerts when keywords are identified in customer outreach and then followed by a transaction for elderly customers. Firms have even set up specific programs to help these vulnerable investors, providing education both internally and externally to help identify risks so they can avoid falling victim to these scams.

As pressure increases to compensate customers who fall victim to scams, most firms are tailoring their approach to deal with these losses on a case-by-case basis. Generally, if vulnerabilities in the firm's control framework were exploited, the respondents typically reimbursed the victims for their losses. If the customer initiated the activity and the control framework performed as designed, respondents indicated that they were less likely to reimburse the customer; however, some firms are erring on the side of caution, as they are wary of the reputational risks from when customers do not feel protected by their financial institution. **Despite the emerging trend in customer scams, there does not seem to be a universally adopted framework among respondents, further exacerbated by the continued lack of guidance from regulators**. As some respondents are seeing an uptick in litigation, each firm must consider the cost of remediation to the customer while balancing their public reputation and commitment to customer loyalty in making these judgment calls.

100% of respondents have noted an increase in financial exploitation, specifically targeting vulnerable investors.

EY | Building a better working world

EY exists to build a better working world, helping to create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

What makes EY distinctive in financial services

Over 84,000 EY professionals are dedicated to financial services, serving the banking and capital markets, insurance, and wealth and asset management sectors. We share a single focus — to build a better financial services industry, one that is stronger, fairer and more sustainable.

US SCORE no. 23164-241US
2311-4384658
ED None

ey.com

Contact us

For further information about our offerings within the fraud and broader financial crime space, please reach out to one of the contacts below or your usual EY US contact.

Walid Raad
Partner
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

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