

Wealth and asset management

Fraud insights point of view

Results and insights

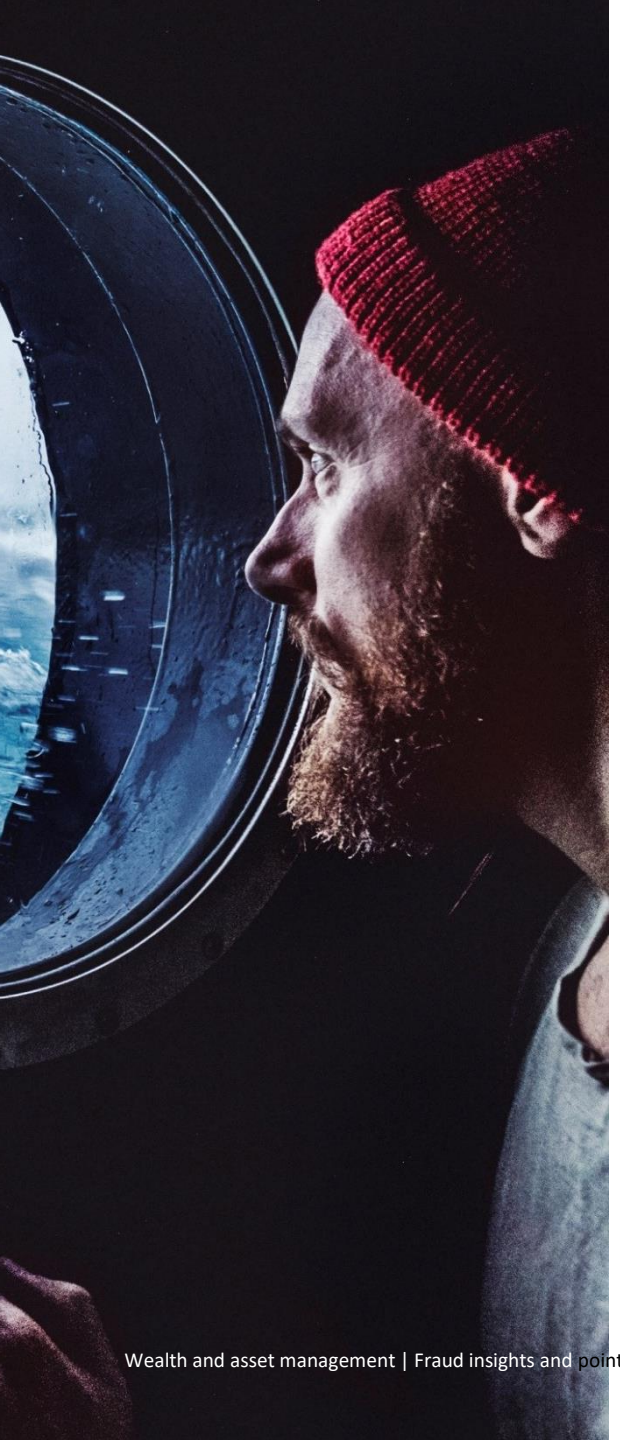
April 2023

EY
Building a better working world

Background

In July 2022, Ernst & Young LLP (EY US) conducted the first wealth and asset management fraud insights point of view exercise to understand the challenges facing our clients and the approaches taken to combat the spike of fraudulent activity currently being experienced. This includes managing staffing needs, identifying technology solutions and innovative fraud investigation management. The following pages summarize the EY US insights, including key takeaways, market themes and emerging trends.





Key themes identified

- New account fraud (NAF) and account takeover (ATO) continue to be the two most prominent fraud concerns for firms. A vast majority of the respondents noted both ATO and NAF are in the top three fraud risks for their organization.
- Teams have seen an influx in fraud volume and a steady increase in average fraud losses over the past three years.
- Many firms ask their existing fraud response teams to manage spikes in fraud volumes. These spikes in volume can put a strain on the existing fraud framework and leave firms vulnerable to large-scale attacks. Over the past three years, some firms have experienced as much as a 500% increase in annual fraud loss from year to year due to large-scale events.
- Some firms have false-positive rates of over 97%, showing fraud teams are potentially inundated with unnecessary alert volumes. As a result, firms have an opportunity to tighten fraud alert intake channels appropriately.
- Firms have a large variety of detective controls used to identify potential fraud red flags; however, they do not have an equally substantial preventative control framework currently in place.
- A majority of firms are utilizing an in-house case management tool, some of which reflect limited functionality, like an inability to report on key metrics accurately. Many tools are also not being leveraged universally throughout the organization, indicating potential inefficiencies between related business lines.
- Firms have expressed concern over their ability to prepare and respond to insider threats. The reporting structure, roles and responsibilities of insider threat programs vary throughout the industry, leading to uncertainty about leading practices.

Fraud losses

60% of firms are currently experiencing an average loss of $1,000 or less, while 40% of firms are averaging a net loss over $5,000 per fraud event. In addition, most firms have seen a spike in fraud since fiscal year 2019. In fiscal year 2019, all firms reported total fraud losses under $10m. Some firms experienced spikes in fraud to over $20m in fiscal year 2020 and $15m to $20m in fiscal year 2022.

60% of firms

are currently experiencing an average loss of $1,000 or less

40% of firms

are averaging a net loss over $5,000 per fraud event

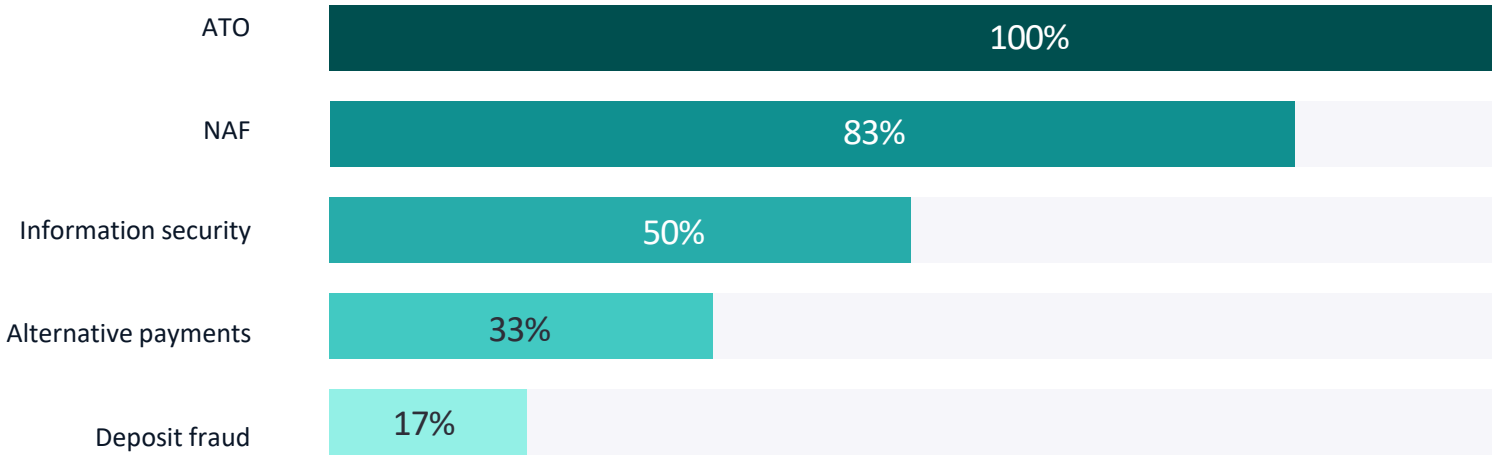


Leading fraud concerns

ATO and NAF are the leading fraud risks facing wealth and asset management firms. Other leading concerns include data breaches, email compromise and information security. Alternative payment methods, cryptocurrency transactions and digital payments also remain at the forefront for many firms.

Between ATO and NAF, **a vast majority of firms expressed that ATO presents a larger threat to the organization.** Typically, firms saw higher volumes of NAF however these fraud incidents average lower net losses per event. Meanwhile, lower volumes of ATO average a much higher net loss per event, as reflected in these insights. Many firms express ATO as their highest loss category.

The chart below reflects the percentage of respondents who expressed concerns about fraud and leading fraud concerns for their organization



83%

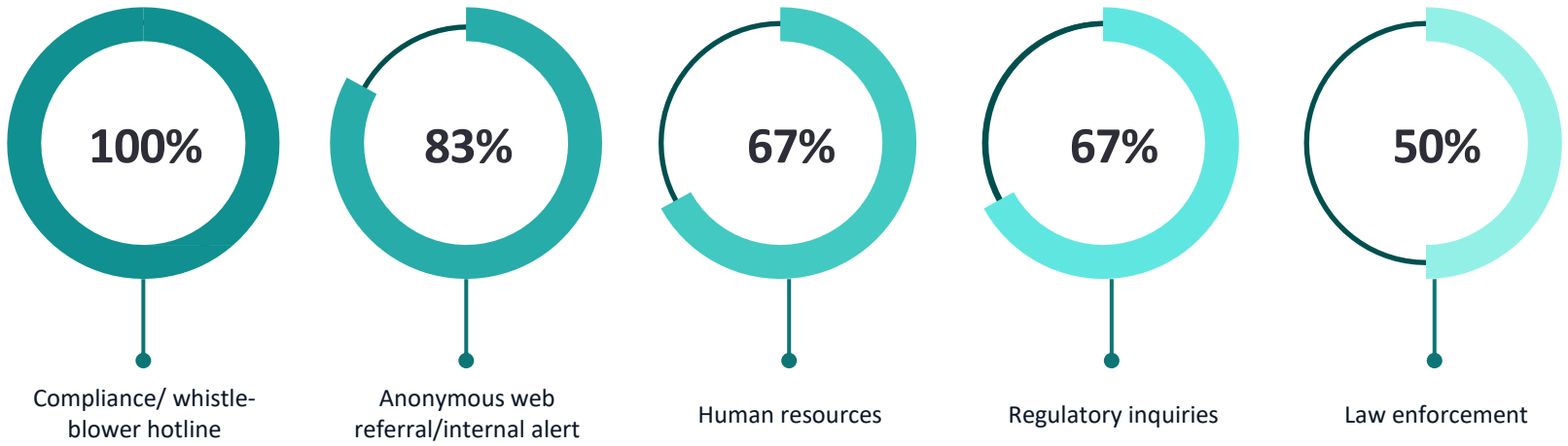
expressed that ATO presents a larger threat of monetary loss to the organization compared to NAF

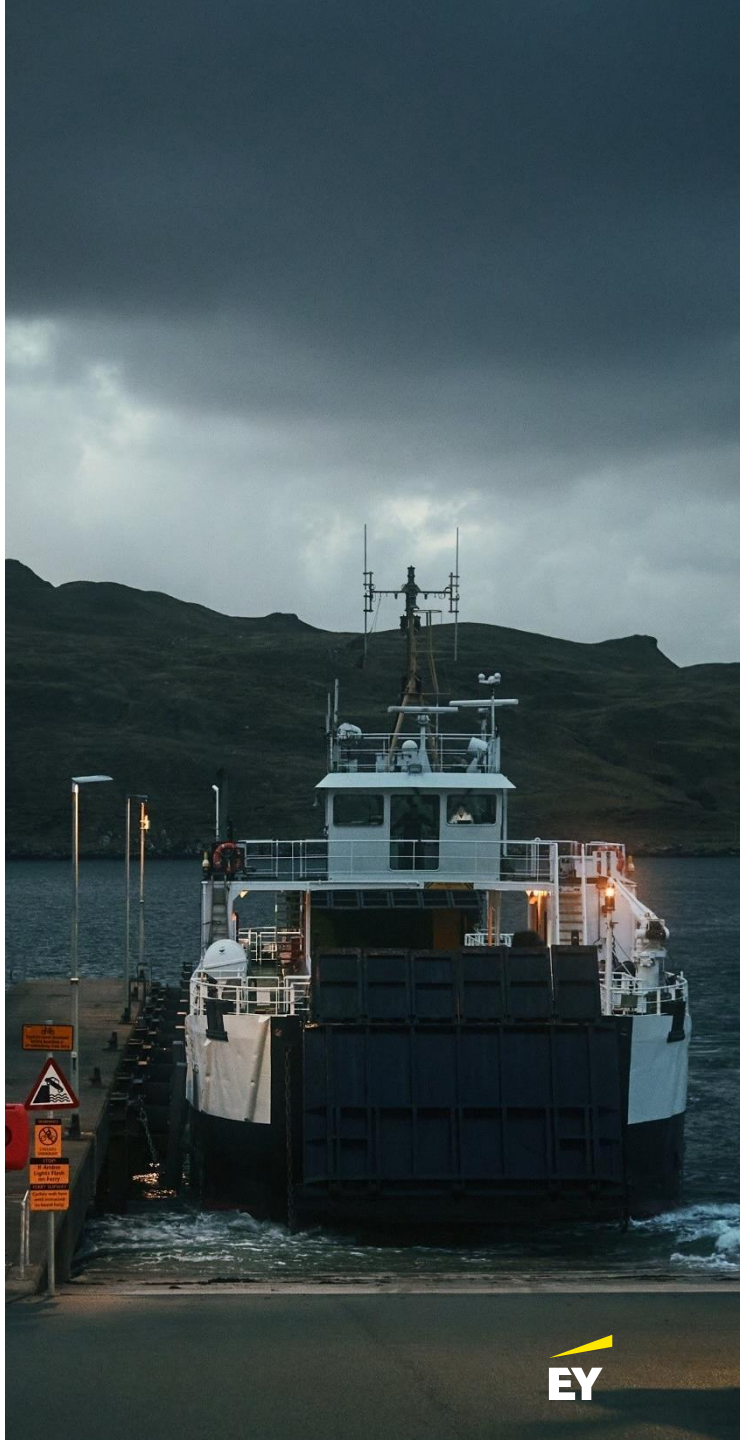
Insider threat teams

The management of insider threat programs was a topic of interest for many firms trying to navigate program enhancements. The responsibility over the insider threat program can vary significantly throughout the industry. For example, **50% of firms have their fraud response teams handle insider threats,** while the other 50% handle insider threats outside of the fraud team. Teams responsible for insider threat programs include global security investigations, financial crimes compliance and general counsel.

> Regardless of where the insider threat program is managed, firms are leveraging similar tools, **focusing on efficient processes, preventative technology and effective intake channels.** Compliance and whistle-blower hotlines, anonymous web referrals and internal alerts are the most common intake channels leveraged to identify insider threat allegations.

Below you can see the percentage of respondents that currently receive tips from the most commonly leveraged insider threat intake channels.







When monitoring for insider threats, programs should include important aspects such as identification of high-risk employees with access to intellectual property and customer information, employees on performance improvement plans, and employees traveling to high-risk jurisdictions.

Insider threat technology

Monitoring internal threats is critical to the timely detection of bad actors. **Insider threat risks exist when employees, contractors or business partners have authorized access to an organization's network system, data and premises, leaving a firm's critical assets exposed.** Internal threats can lead to monetary and reputational harm. 67% of respondents are using tools to proactively monitor for internal threats.

Firms that proactively monitor for internal threats use a combination of internal and external tools to conduct pattern-based analysis and behavior analytics to detect suspicious or abnormal behavior. These algorithms tend to be reviewed and recalibrated periodically as a result of confirmed insider threats or near misses.

25%

of respondents leverage only internal monitoring tools

75%

of respondents leverage both internal and external monitoring tools

Strategic initiatives

Most firms expressed they have the authority and budget to invest in new hires and technology. In addition, all firms expressed their focus and investment in technology in the future state, including modernization efforts, as well as enhancements to the existing controls framework. Key areas of technological investment include case management tools, social media scrubbing, web session monitoring and two-factor authentication.



> “Controls that are in place are going through an enhancement process. We believe our industry is behind traditional banking institutions in regard to proactive and preventative capabilities.”
>
> Global Head of Fraud Investigations

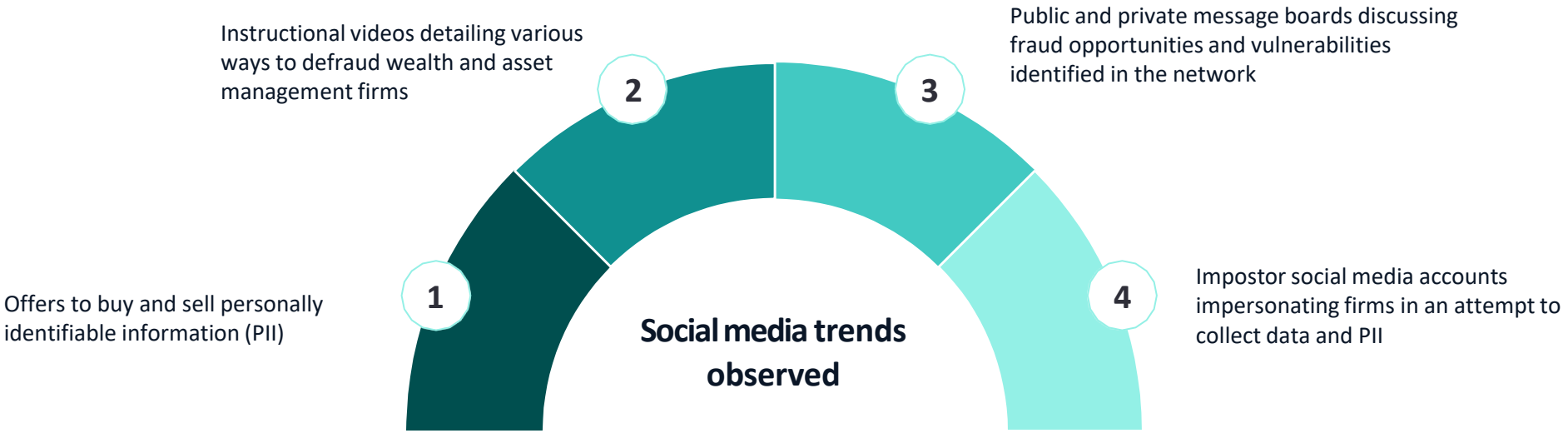
Social media searches

A vast majority of the firms currently employ some form of social media or dark web searches. These searches are a useful tool that helps identify online discussion boards created to share customer information and preferred methods for infiltrating industry networks.

By performing these searches, firms have identified bad actors attempting to infiltrate their networks and sell customers' personal information. **Once fraud trends are identified, preventative controls are put in place before the organization's business operations can be targeted.**

Firms have also been sharing information to shed light on these schemes and prevent these schemes and fraudsters from gaining any traction throughout the industry.

Firms work with law enforcement and site administrators to pursue legal action and remove postings that target the organization.



Technology capabilities

Data analytics has proven to be crucial in preventing and detecting fraud. Firms are leveraging various data analytics tools, including **automated red flags and business rules, exception reporting and behavioral analytics.** These tools are especially useful when helping firms combat bot activity and dormant accounts. As bot activity can strike quickly and in high volumes, firms heavily leverage behavioral analytics, like tracking the number of open web sessions and implementing session timeout restrictions to detect and prevent bot activity early.

> Dormant accounts present a different problem as they can be idle for extended periods and begin transacting with no prior account history to evaluate them against. Firms are generating reports and conducting retroactive analysis to identify inactive accounts; however, generally, they are looking to focus their efforts on more proactive measures in the future state.

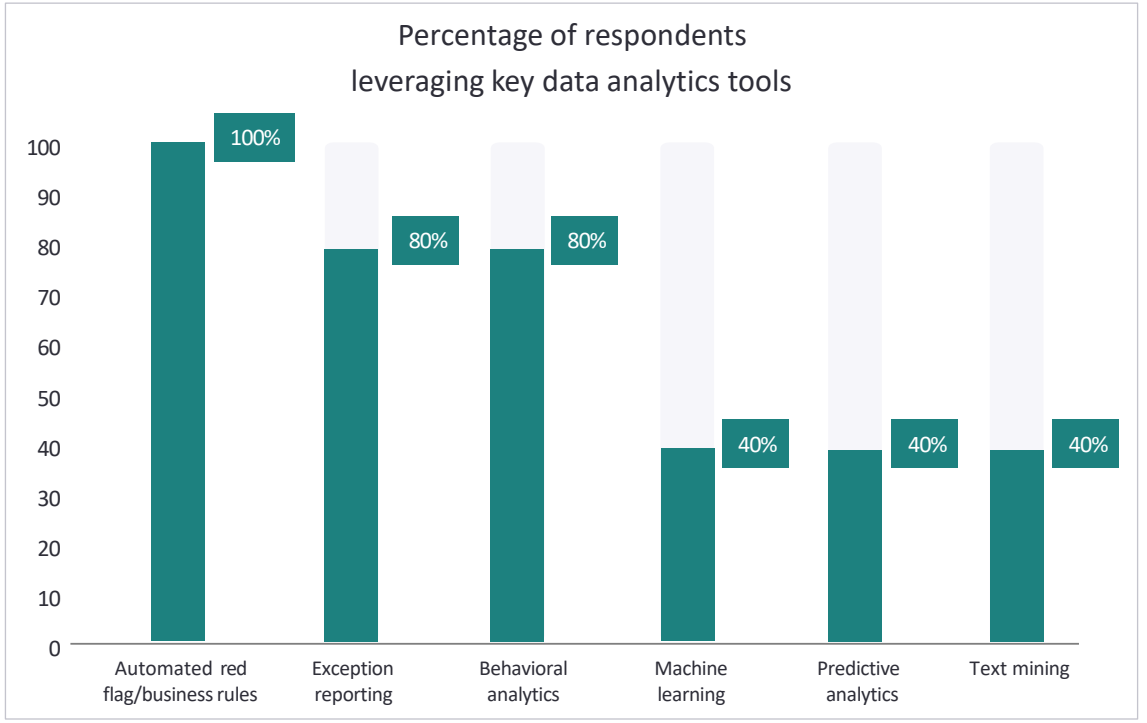
Useful tactics leveraged to combat common fraud risks

Address dormant accounts

- Freeze or block accounts after a specified number of months of inactivity
- Run reports and/or conduct retroactive analysis
- Generate alerts for unexpected account activity

Prevent bot attacks

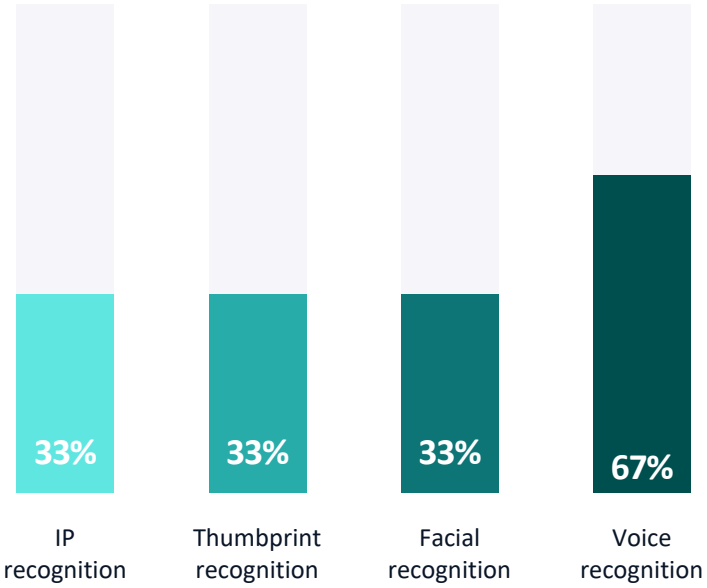
- Behavioral analytics
- Session timeout if multiple open sessions detected
- Third-party vendors to distinguish between human and automated access to websites



Enhanced authentication

Only 50% of firms are currently using biometrics or device metrics as an authentication criteria when using their networks. Preventative controls such as facial, thumbprint, voice and IP recognition are all valuable tools that help protect firms and their customers from unauthorized access to their profiles. Many firms are utilizing third-party validation tools to combat synthetic identity fraud.

Percentage of respondents leveraging most common authentication methods

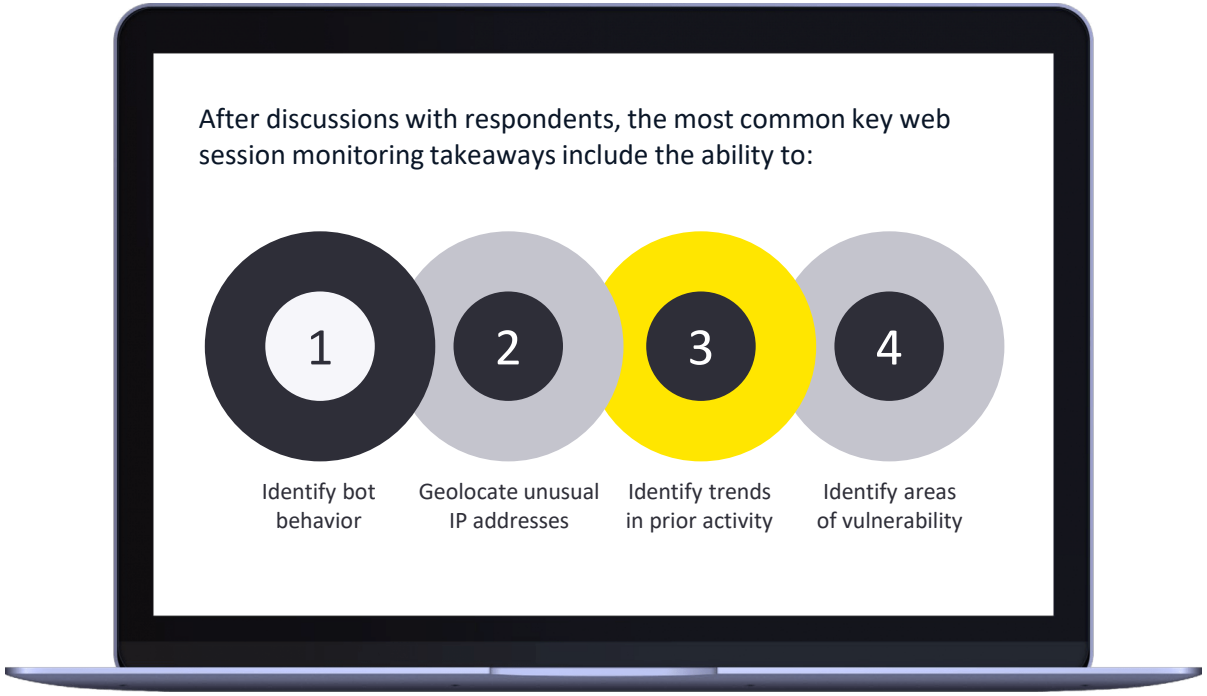




> “Proactive technology spending and hiring are tough sells in the current environment. The team is not adverse to these changes, but it can be difficult to accomplish currently.
>
> Global Head of Cyber and Fraud Prevention

Web session monitoring

Firms have expressed how **web session monitoring is essential in the effort to identify fraud trends and help build a sustainable preventative control framework.** Once a fraud pattern or trend has been identified in the network, teams can perform a deep dive into the activity, determining where accounts are being opened from, tracking fraudsters' keystrokes and monitoring their web behavior.

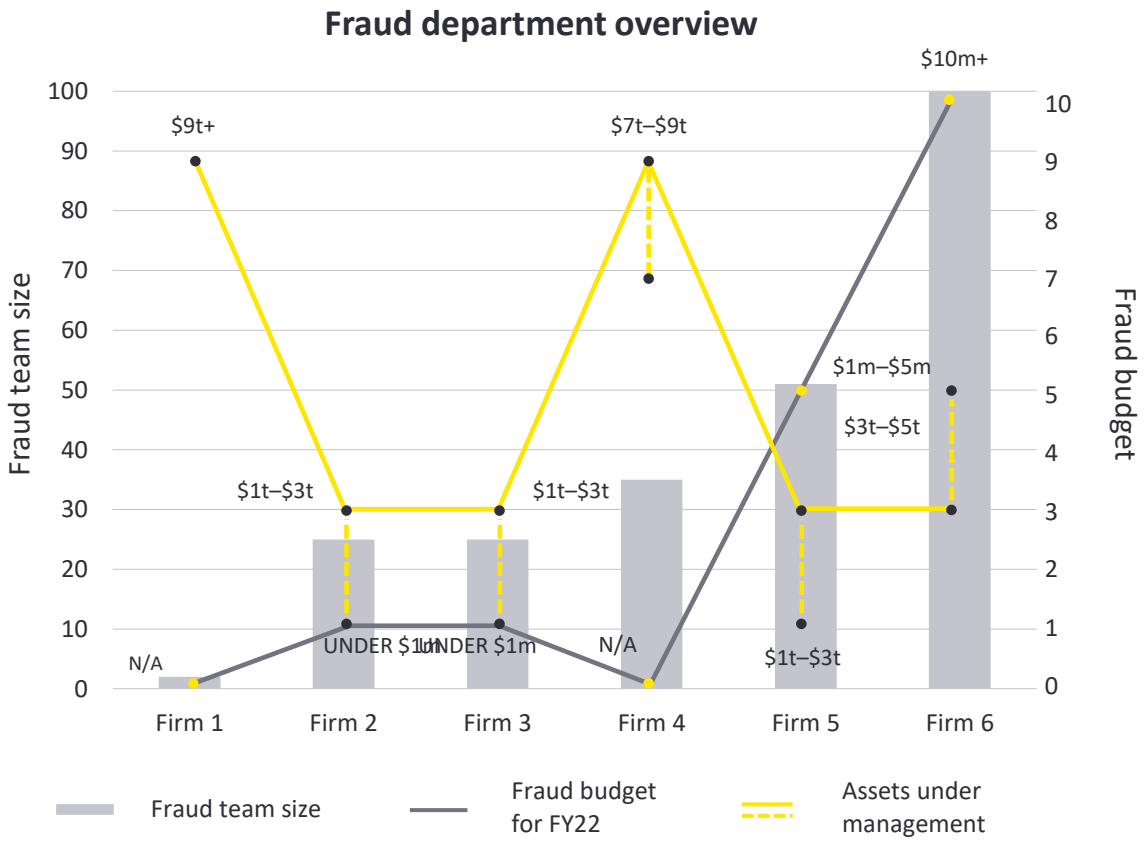


Web session monitoring not only allows the business to understand the scope of the fraud attacks occurring, but also allows the business to set up preventative controls to block future activity of identified fraudulent patterns.

Fraud departments

Fraud departments sit within various pillars throughout the polled wealth and asset management organizations. Fraud is a stand-alone pillar within some businesses, while others house their fraud departments within risk, legal, compliance or operations. A majority of fraud departments sit as a second line of defense. Additionally, 50% of fraud response teams consist of over 35 professionals, some as large as 100 employees.

The chart below reflects the differences between the size of the fraud response team, the assets under management and the fraud budget for fiscal year 2022 for a sample of wealth and asset management firms. In general, there is an increase in the team size and budget as assets under management increase; however data reflects some inconsistency throughout the industry.





Key takeaways

As bad actors continue to find new and complex ways to share customer information and gain unauthorized access to customer accounts, **firms must take a look at the current standing of their fraud program, assessing the ways they identify internal and external threats and the controls in place to prevent fraud.** Wealth and asset management firms have made and continue to make a substantial investment in their people and technology to bolster their fraud framework against the recent increases in fraud observed. Firms must continue to work toward a mature and robust fraud program, including a **strong preventative control framework, a defined insider threat program and optimized intake channels to operate effectively and efficiently.**

The future of fraud

EY US point of view

Based on our conversations with wealth and asset management firms and the current market trends we observed, we suggest the areas below will become a key focus as firms look to continue enhancing their existing fraud framework.

Firms are making investments to enhance their existing fraud infrastructure and preventative control framework, further integrating machine learning, automated alert generation and behavioral analytics to better inhibit bad actors from gaining access to their network. Specifically, machine learning and behavioral analytics will assist in identifying fraudulent patterns, for which agile preventative controls can be developed and adjusted to fit the most current fraud trends observed.

A comprehensive and integrated insider threat program will be necessary to protect against potential exposure and future vulnerabilities. Firms are assessing their existing insider threat framework maturity and determining if the program is fully integrated into the enterprise risk management strategy. In addition, insider threat programs are being designed to proactively detect insider threat activities with risk indicators in place to focus on higher-risk employees (e.g., those with access to confidential information, or low-performance indicators).

Social media and dark web investigations will become widespread and commonplace across the industry. Firms will continue to heavily leverage a combination of third-party vendor tools and in-house resources as effective resources to identify when and where bad actors have identified vulnerabilities and where they are coordinating future attacks.

Providing additional fraud training and raising awareness will further bolster a firm's preventative framework and assist in combating fraud. Enhancing education for customers and employees on how to spot fraud red flags internally and externally, how to defend themselves against bad actors and where to go if they identify potential fraud can create operational efficiencies for the business and help optimize manual alert intake channels.

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



Emma Monaghan
Principal
Ernst & Young LLP
+1 212 773 1577
emma.monaghan@ey.com



Lou Bladel
Managing Director
Ernst & Young LLP
+1 202 327 7426
lou.bladel@ey.com



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



EY | Building a better working world

EY exists to build a better working world, helping 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.



EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. EY member firms do not practice law where prohibited by local laws. For more information about our organization, please visit ey.com.

Ernst & Young LLP is a client-serving member firm of Ernst & Young Global Limited operating in the US.

© 2022 Ernst & Young LLP.
All Rights Reserved.

SCORE no. 17213-221US
2207-4071898
ED None

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax, legal or other professional advice. Please refer to your advisors for specific advice.

ey.com