Financial Crimes Services and Fraud Prevention

Benchmarking Study

LIMRA

Navigate With Confidence

Contact Information

Russell Anderson, CFE
Head of Fraud Prevention and Compliance Solutions
randerson@limra.com

Sharyn Kessler
Product Manager, Fraud Prevention and Compliance Solutions
skessler@loma.org

Contents

Figures

Tables

About the Study

Financial Crimes Services and Fraud Prevention Benchmarking Study

As fraudsters continue to expand their capabilities by adopting increasingly accessible technologies, including AI and fraud as a service (FaaS) models, life and retirement carriers must respond by increasing their investments in fraud prevention, authentication, and analytics

This benchmarking synthesizes how peers organize, govern, measure, equip, and evolve their financial crimes and fraud prevention programs. It covers organization and staffing, maturity, governance and reporting, technology and spend, authentication, fraud trends, training and awareness, law enforcement coordination, risk assessment, challenges, and 2026 outlook.

Methodology

The Financial Crimes Services and Fraud Prevention Benchmarking Survey questionnaire was distributed via email in December 2025 to 136 companies. Data collection concluded in February 2026, with participation from 60 companies — a 44 percent response rate and the highest in six years. Among the respondents, 22 companies participated consistently each year from 2020 through 2026. See Appendix A for the list of participants.

Executive Summary

The 2025 Financial Crimes and Fraud Prevention Benchmarking Survey signals a pivotal shift for the insurance and retirement services industry. Fraud risk is no longer defined by isolated incidents or single channels — it is persistent, technology enabled, and increasingly human centric. As organizations look ahead to 2026, the findings point to both heightened urgency and a narrowing margin for delayed action.

Fraud will remain a strategic enterprise risk, not an operational issue.

With organizations experiencing nearly all major fraud types and attacks increasingly spanning multiple channels, fraud prevention must be treated as a core risk discipline integrated across operations, technology, compliance, and customer experience. Programs designed primarily for detection and response will struggle as fraudsters move faster, scale broader, and exploit trust based interactions.

AI-enabled fraud will accelerate faster than defensive adoption.

Fraudsters' use of AI — particularly in text and voice impersonation — has already outpaced most organizations' ability to respond. In 2026, AI-enabled fraud should be assumed, not anticipated. Companies that remain in evaluation or pilot phases risk falling further behind adversaries that are already operationalizing these tools at scale.

Voice and servicing channels will be the highest risk exposure.

The convergence of rising impersonation attacks and persistent reliance on basic authentication in call centers and interactive voice response (IVR) creates a material vulnerability. In 2026, organizations that do not modernize voice channel controls should expect increased account takeover, social engineering losses, and customer-trust erosion.

Identity assurance will define fraud prevention effectiveness.

Stronger authentication — across customers, agents, and employees — will be the single most impactful control area in 2026. This includes consistent, risk based authentication across channels, improved identity verification during servicing events, and tighter controls around high risk transactions such as withdrawals and bank account changes.

Seniors and vulnerable adults will remain a focal risk — and reputational amplifier.

Fraud targeting vulnerable populations is no longer episodic; it is chronic and growing. In 2026, regulatory scrutiny, reputational exposure, and customer expectations will increasingly hinge on how well organizations protect and educate these groups — making customer facing prevention programs a strategic necessity, not an optional enhancement.

The capability gap between large and small organizations will widen.

Larger organizations are accelerating investment in staffing, AI, and advanced analytics, while smaller firms are more likely to hold budgets flat. Without creative approaches — such as shared intelligence, industry utilities, or targeted investments — smaller organizations may face disproportionate exposure relative to their ability to respond.

Foundational readiness will matter as much as new tools.

Data quality, integration, governance, and skilled resources are now gating factors for progress. In 2026, organizations that focus solely on acquiring new technology without strengthening these foundations will struggle to realize meaningful risk reduction.

Governance is strong at the top, but risk visibility must move closer to the front line.

While board and executive oversight is well established, fraud intelligence is not consistently flowing downward where early warning signals appear first. Strengthening two way communication between leadership and frontline teams will be critical to faster detection and response.

Customer education will emerge as a differentiator.

Despite rising confidence scams and impersonation, most organizations still under invest in customer awareness. In 2026, proactive education — especially for vulnerable customers — will differentiate leaders from laggards and serve as a force multiplier for internal controls.

Industry collaboration will remain essential — but insufficient on its own.

Shared intelligence and law enforcement partnerships continue to be a strength, yet respondents clearly recognize that collaboration must be paired with faster technology adoption and execution. The industry's ability to standardize metrics, share insights, and act decisively will shape collective resilience in 2026.

Bottom line:

2026 will reward organizations that move beyond maintaining "operational" fraud programs and instead build adaptive, intelligence driven, and customer aware defenses. Fraud prevention is no longer about keeping pace — it is about staying ahead in an environment where trust, identity, and technology are the primary battlegrounds.

Key Findings

1. Fraud incidents continue to rise across nearly all categories.

Companies experienced increases in the majority of fraud types, with **account takeover (unrelated)** and **senior/vulnerable adult exploitation** among the most frequently rising threats. Fraud incidents involving senior and vulnerable adults (both related and unrelated) continue to rank as one of the top five increasing fraud incidents year over year, indicating a continued persistence and growing threat to this demographic.

2. AI-enabled fraud is accelerating at an unprecedented pace.

The share of companies reporting no AI-enabled attacks has fallen sharply — from **58 percent to just 24 percent in one year**. Reports of AI-generated or altered correspondence jumped from **25 percent to 59 percent in a single year**, while AI-based voice impersonation increased from **30 percent to 54 percent**, highlighting a rapidly evolving threat landscape.

3. Fraud prevention teams remain small but are growing steadily.

Fraud prevention staffing has grown steadily since 2020 with a median of **four staff in 2020 to 11 staff in 2025**, and **42 percent** of companies expect further staff increases, signaling sustained investment in fraud-fighting capacity.

4. Most organization's financial crimes and fraud prevention programs operate at an "operational" maturity level.

In 2025, **72 percent** classified their programs as operational, with only 12 percent reaching "optimal," showing progress yet highlighting the gap between functional and fully mature programs.

5. Governance has strengthened, but frontline reporting lags.

While **83 percent** report regularly to senior management and executive leadership, only 29 percent provide consistent reporting to frontline managers — an ongoing visibility gap.

6. Peer fraud metric sharing is widely valued but constrained by standardization gaps.

While **93 percent** of companies see value in sharing fraud metrics with peers, lack of shared definitions and internal alignment remain major barriers to broader data sharing.

7. Fraud risk assessments are becoming more routine, but risk tolerance remains unclear.

While most companies conduct periodic fraud risk assessments and **79 percent** update their programs as a result, nearly half **(46 percent)** still lack a formally defined fraud risk appetite, limiting consistent, risk based decision making.

8. AI adoption for fraud prevention is progressing but remains largely preoperational.

While fewer companies remain in the awareness stage (**33 percent**, down from 49 percent in 2024) and more have advanced to evaluation (**35 percent)** or experimenting (17 percent), no organizations have reached a transformative level of AI maturity, with resource constraints (62 percent), data quality and access issues (53 percent), and skills gaps (47 percent) continuing to limit scalable deployment.

9. Fraud prevention spending is stabilizing as a core cost, while AI investment accelerates but remains secondary for most firms.

Budgets are largely flat or increasing with no planned reductions — signaling sustained commitment — yet most companies still treat AI as an incremental investment, particularly larger organizations, potentially widening capability gaps as AI-enabled fraud grows more sophisticated.

10. Authentication enhancements remain a top priority across channels.

Companies increasingly deploy advanced authentication — OTP, device identification, biometrics — especially for digital access, with **66 percent** using advanced methods for mobile app login.

11. Training for employees is strong, but customer education is a critical gap.

While **98 percent** require employee fraud awareness training, **73 percent** do **not** regularly provide fraud education to customer groups — despite customers being primary targets for social engineering.

12. Converging operational pressures are reshaping fraud program priorities.

Organizations report increasing difficulty balancing a seamless customer experience with effective fraud vigilance (51 percent), alongside persistent challenges in authentication and identity security (47 percent) and the accelerating impact of AI on fraud risk (44 percent). To address these pressures, insurers are accelerating investment in technology and vendor solutions and placing greater emphasis on workforce enablement.

13. AI enabled identity attacks will dominate future fraud risk.

Account takeover and AI-driven fraud are expected to be the most significant challenges in 2026, intensifying organizational focus on stronger authentication controls and AI-enabled detection and prevention capabilities.

14. Collaboration is strong, but technology adoption is lagging.

While insurers view industry collaboration as a key strength, nearly half believe the insurance and retirement sector is falling behind other industries in adopting advanced, technology-driven fraud fighting capabilities.

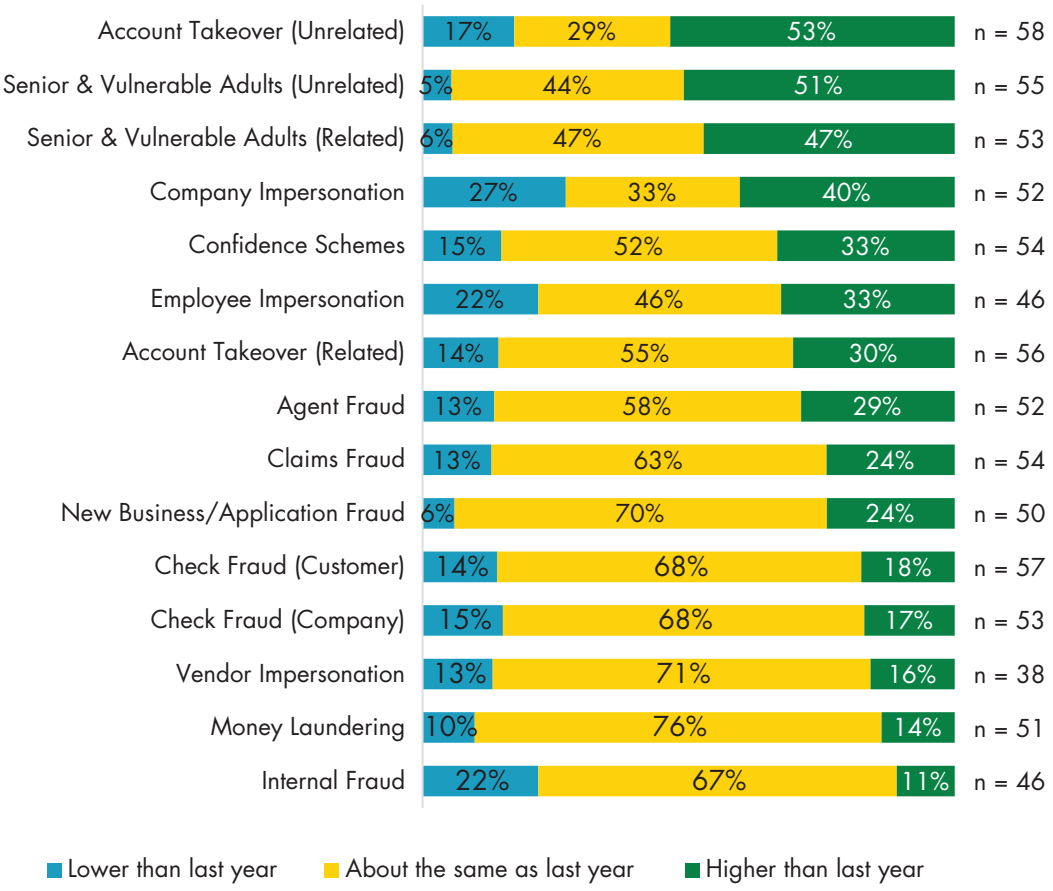
Fraud Trends

The upward trend in fraud incidents continues across most categories (see Figure 1). In 2025, companies assessed all 15 types of fraud incidents, indicating whether each had increased, remained the same, or decreased compared to the prior year. On average, companies experienced 13 of the 15 fraud types.

With the exception of internal fraud, companies reported more increases than decreases across all confirmed fraud incident types. Over half of companies reported increases in account takeover (unrelated) (53 percent) and Senior and Vulnerable Adult (unrelated) fraud incidents (51 percent). Money laundering showed the least year over year change, with 76 percent of companies reporting similar levels to 2024. Twenty-seven percent of the companies reported a decline in company impersonation.

It is important to note that a fraud "incident" reflects attempted activity and does not indicate whether those attempts were successful.

Figure 1 — Percentage of Companies Reporting 2025 Trends in Fraud Incident Types



Note: Due to rounding, percentages may not total 100.

Confirmed Fraud Incidents Over the Years

The analysis of confirmed fraud incidents from 2021 to 2025 reveals several notable trends that illustrate the shifting fraud landscape. Companies have continued to closely monitor a wide range of fraud types, and the results highlight both emerging concerns and areas of relative stability. Figure 2 shows fraud incident rankings from 2021 to 2025, demonstrating how the prevalence of different fraud types has evolved over time.

Incidents involving senior and vulnerable adults — both related and unrelated — have consistently ranked among the top five increasing fraud types each year. This persistent upward trend underscores the heightened and growing risks facing these populations and signals the need for targeted protective measures.

Company impersonation rose sharply, jumping from rank eleven to rank four; however, performance varied notably by company size, with 75 percent of large companies reporting an increase in this type of fraud. Similarly, employee impersonation advanced from rank 12 to rank six, with 56 percent of large companies indicating rising incidents.

Check fraud continues to decline across both customer and company accounts, suggesting that enhanced controls are proving effective — or that fewer people are using checks as a payment method. However, this downward trend also signals a likely shift in fraud activity toward other channels, underscoring the need for broader, cross channel protection strategies.

Conversely, internal fraud and money laundering have remained among the least frequently reported increases, suggesting relatively stable incidence levels.

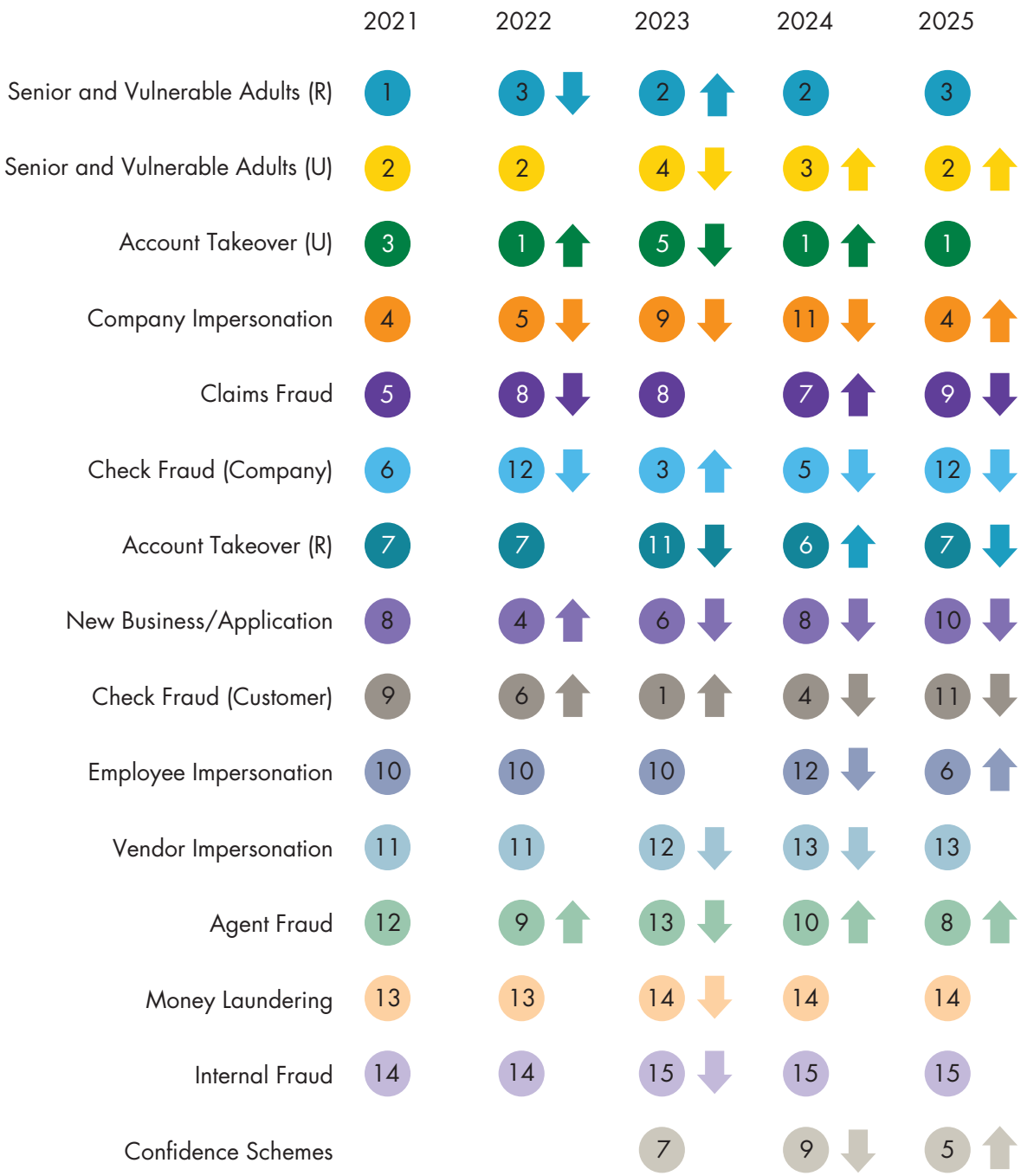
Overall, the chart underscores the importance of continued vigilance and adaptability in fraud prevention. As fraudsters refine their tactics, companies must stay proactive in detecting emerging risks and enhancing safeguards to protect their organizations, customers, and vulnerable populations.

Strategic Insight:

Fraud trends in the life insurance and retirement services industry from 2021–2025 show a clear shift toward **trust based and socially engineered schemes**, particularly those targeting seniors and vulnerable adults. Rising company and employee impersonation highlights increasing exploitation of trusted brands and internal authority, while declines in check fraud suggest risk is migrating to digital and servicing channels.

To remain resilient, organizations must strengthen identity controls, enhance behavioral monitoring, and expand protections for vulnerable policyholders and account holders.

Figure 2 — Most Reported Fraud Incident Increases by Type Over the Years (Most to Least Reported)



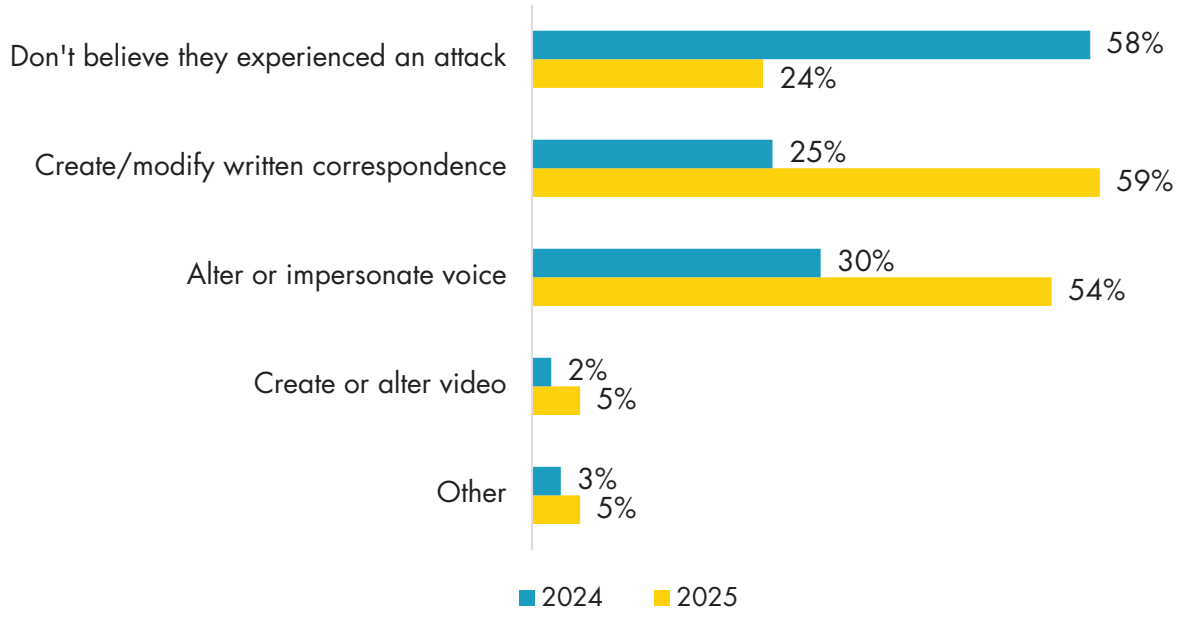
Emerging AI-Related Fraud Incidents

Reports of fraud attacks involving AI have shifted dramatically. Only 24 percent of companies believe they did not experience an AI-enabled attack, down from 58 percent the year before.

Fifty-nine percent of organizations have now encountered AI-generated or AI-modified fraudulent correspondence, up sharply from 25 percent last year. Additionally, 54 percent have faced attacks in which AI was used to alter or impersonate a voice, compared with 30 percent in 2024. Attacks involving AI-created or AI-manipulated videos have remained relatively low at five percent.

Together, these findings show that AI-enabled fraud is no longer emerging — it is already widespread and increasingly concentrated in text and voice channels. While video based attacks remain limited for now, the rapid growth in AI-driven correspondence and voice impersonation underscores the need for organizations to prioritize defenses where risk is highest and most immediate (see Figure 3).

Figure 3 — Prevalence of AI-Enhanced Fraud Tactics Against Organizations



Strategic Insight:

AI-enabled fraud has rapidly become a **mainstream and material risk** for the life insurance and retirement services industry, with a sharp rise in AI-generated correspondence and voice impersonation directly targeting policyholders, advisors, and service operations. The concentration of attacks in **text and voice channels** reflects fraudsters' focus on exploiting trust based interactions central to policy servicing and retirement distributions.

Insurers and retirement providers must urgently prioritize defenses in these high-risk channels, strengthening identity verification, communication controls, and employee awareness to preserve customer trust and fiduciary integrity.

Organizational Structure and Staffing

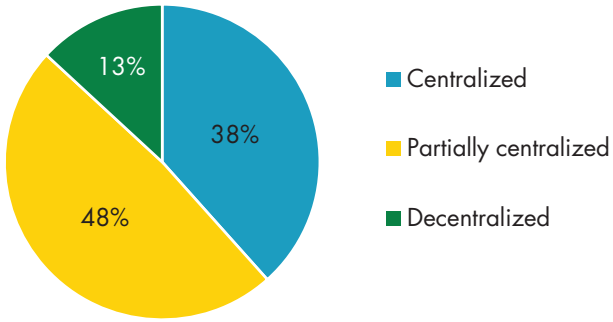
Structure

In 2025, companies continue to adopt a range of organizational structures for managing financial crimes and fraud prevention. There is no one size fits all model; each organization shapes its structure around its culture, operating model, staffing, and product offerings. What matters most is the ability to stay adaptable as threats evolve.

Nearly half of carriers (48 percent) use a partially centralized model, which allows them to maintain strong enterprise wide standards while still enabling flexibility at the line of business level. This balance helps companies address specialized or emerging fraud risks without sacrificing consistency. Another 38 percent operate fully centralized programs, benefiting from unified oversight, coordinated analytics, and streamlined decision making — though this structure can sometimes limit local responsiveness when fraud patterns differ across products or markets. The remaining 13 percent use decentralized structures, gaining agility and faster response times within business units, but also facing challenges such as inconsistent practices and limited visibility into cross channel fraud patterns.

Together, these structures reflect the varying strategic priorities across organizations, as each seeks the right mix of consistency, agility, and visibility to defend against a rapidly changing fraud landscape (see Figure 4).[1]

Figure 4 — Prevalence of Organizational Structures



Note: Due to rounding, percentages may not total 100.

[1] See Appendix for definitions of organizational structures.

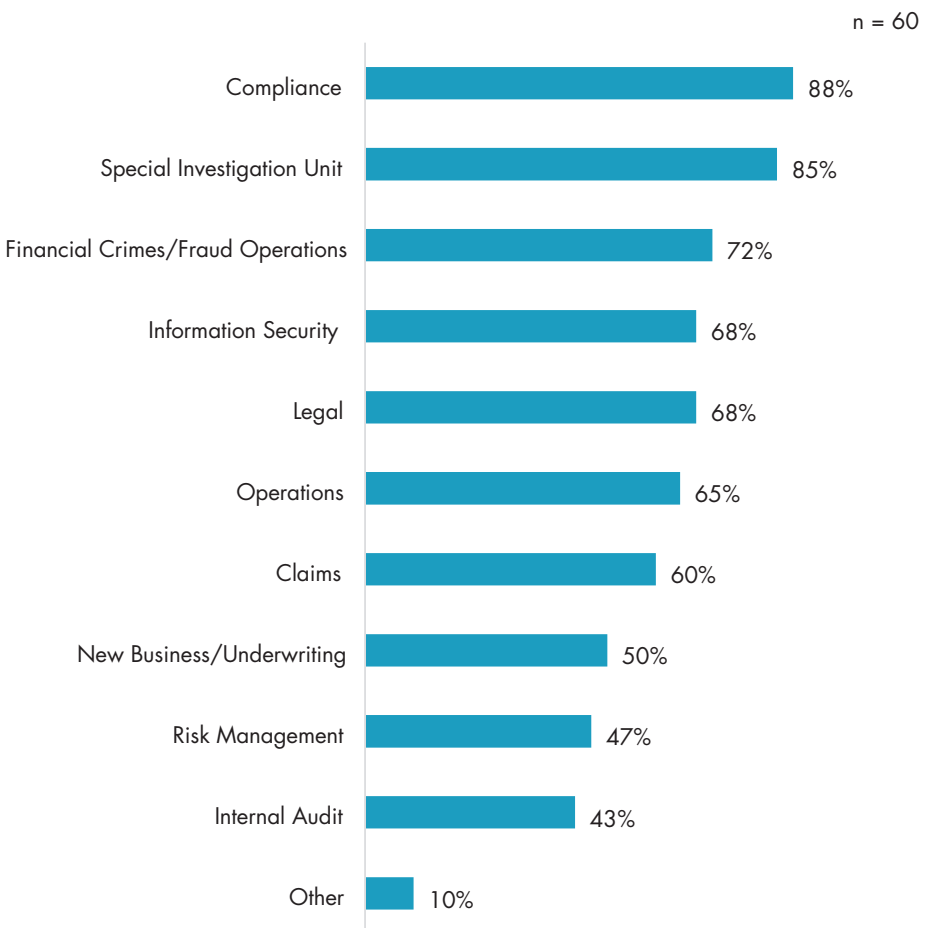
Departmental Roles and Reporting

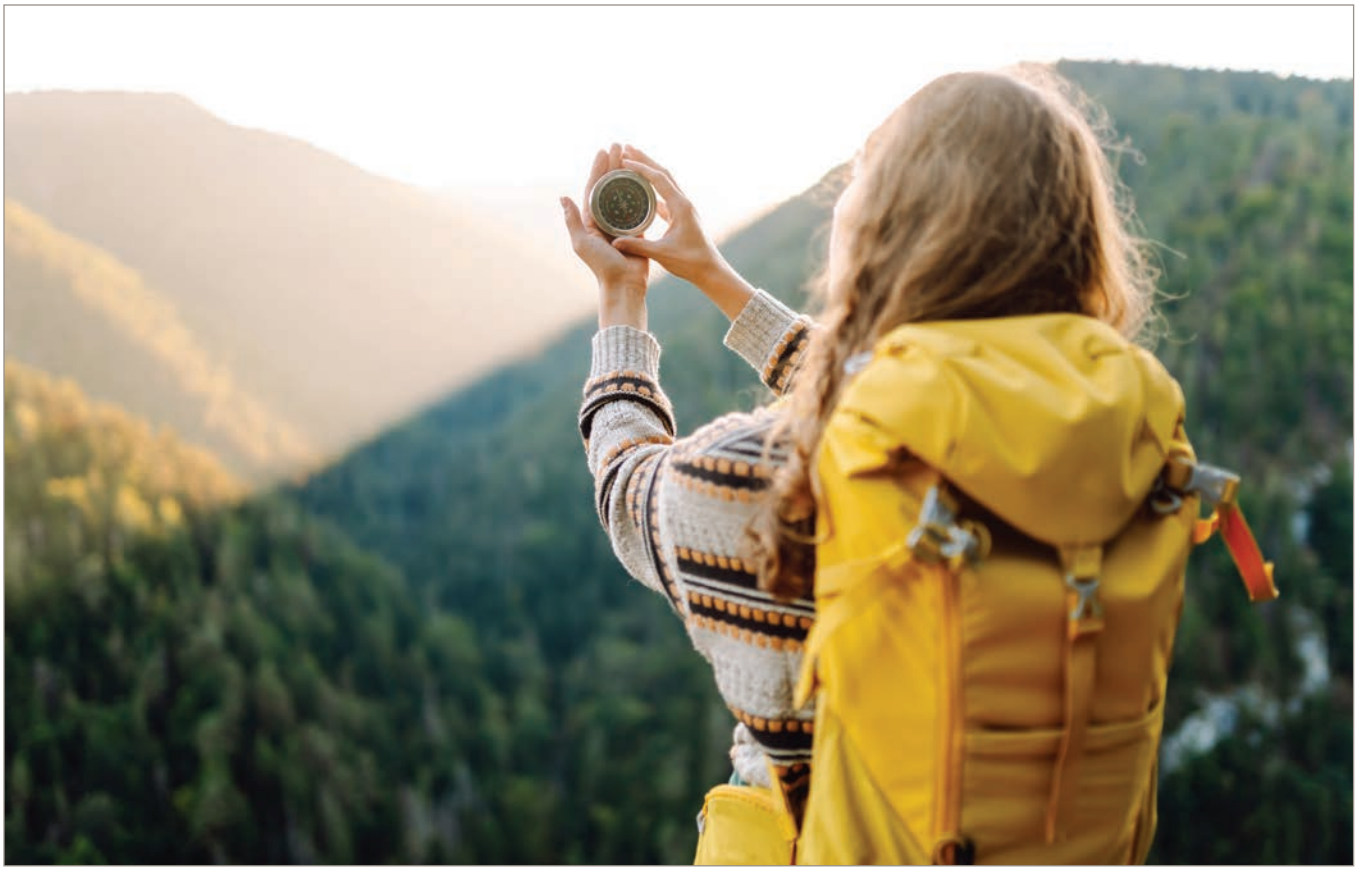
Regardless of how companies structure their financial crimes and fraud prevention programs, an average of seven departments are actively involved, reflecting the cross functional nature of fraud risk management. The most engaged groups are Compliance (88 percent) and Special Investigation Units (85 percent), indicating that regulatory oversight and investigative expertise remain central to effective prevention efforts. In contrast, departments such as Internal Audit (43 percent) and Risk Management (47 percent) are involved less frequently, which may limit organizations' ability to take a more holistic, enterprise wide view of emerging threats. (Figure 5) This distribution highlights a continued need for stronger cross department coordination, ensuring that fraud prevention strategies draw on diverse perspectives — from control testing and risk assessment to investigations and compliance monitoring.

Primary responsibility for the Financial Crimes and Fraud Prevention Management Program is distributed relatively evenly across Special Investigation Units (33 percent), Financial Crimes/Fraud Operations (28 percent), and Compliance (25 percent). Nearly half of all companies (48 percent) have the program reporting directly to the Compliance department, with an additional 20 percent reporting to Legal.

Taken together, these patterns show that while functional ownership varies, organizations overwhelmingly rely on Compliance and Legal for ultimate oversight.

Figure 5 — Teams With an Active Role in the Financial Crimes and Fraud Prevention Management Program





Strategic Insight:

Fraud operating models in the life insurance and retirement services industry increasingly reflect a strategic balance between enterprise wide consistency and business level agility, with partially centralized structures emerging as the most common approach. While fraud prevention remains inherently cross functional, oversight is still concentrated within Compliance and Legal, reinforcing regulatory and fiduciary priorities but potentially limiting enterprise wide risk visibility.

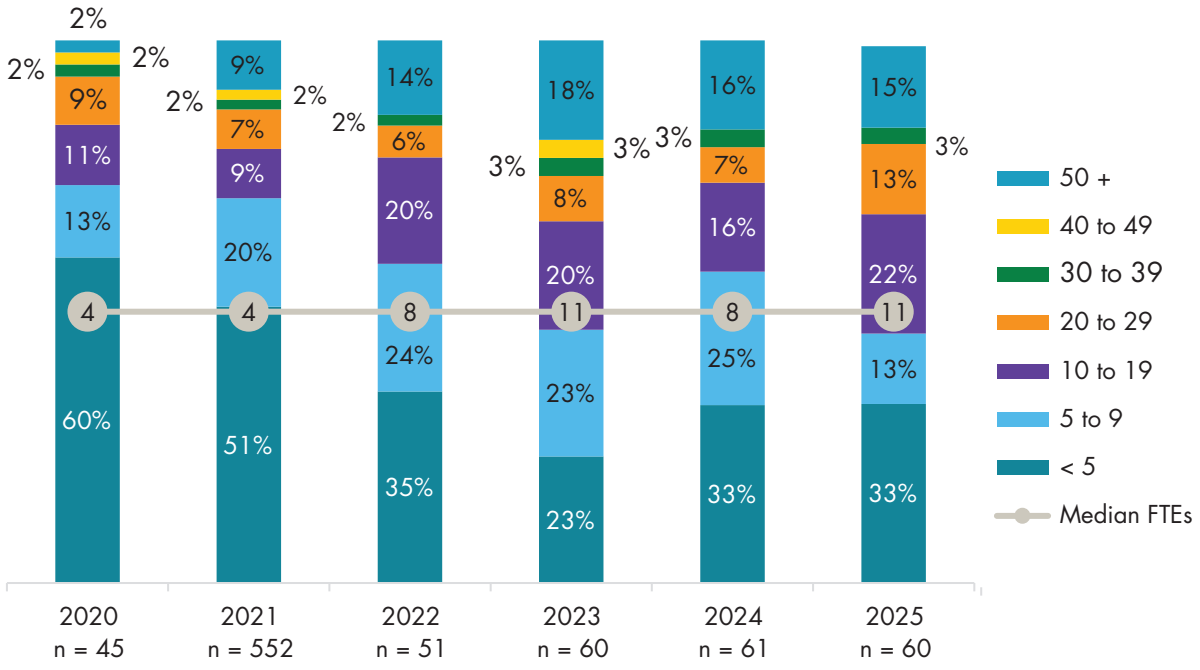
Organizations that strengthen collaboration across Compliance, Investigations, Risk Management, and Internal Audit will be better positioned to adapt, share intelligence, and maintain cross channel visibility as fraud threats continue to evolve.

Staffing Trends and Projections

In 2025, the size of teams supporting financial crimes and fraud prevention programs remains relatively small, with 46 percent of programs operating with fewer than 10 full time equivalents (FTEs). As expected, team size varies considerably based on company size. Nearly half of organizations with more than 5,000 employees (47 percent) have teams of 50 or more FTEs, while 78 percent of companies with fewer than 500 employees rely on teams of fewer than 5 FTEs. This wide disparity reflects the differing levels of investment and organizational capacity across the industry — highlighting that larger companies are better positioned to support specialized, resource intensive fraud prevention efforts, while smaller organizations may face greater constraints in keeping pace with increasingly complex threats.

Over the past six years, staffing levels have shifted significantly (see Figure 6). Programs operated with a median of just four FTEs in 2020–2021, indicating relatively limited resourcing. By 2022 and 2024, staffing had doubled to a median of eight FTEs, reflecting increased investment in financial crimes and fraud prevention. Levels peaked at 11 FTEs in 2023 and 2025, suggesting heightened operational demands and a continued priority on strengthening these programs.

Figure 6 — Full-time Equivalents (FTEs) Currently Supporting the Program (2020–2025)

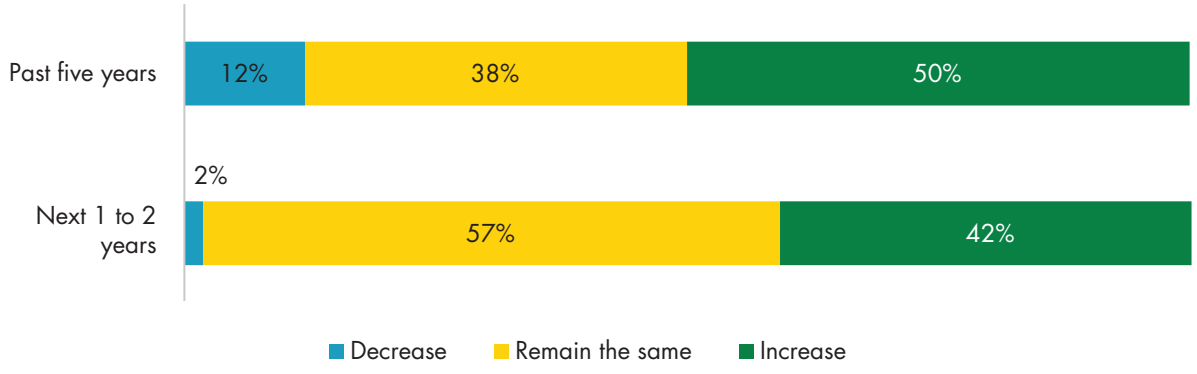


Over the past six years, financial crimes and fraud-prevention programs have seen notable shifts in staffing levels. Half of all programs reported a slight or significant increase in staff, reflecting growing organizational recognition of the need for expanded fraud fighting capacity. In contrast, only 12 percent experienced a slight decrease. These trends align with earlier findings and point to an overall expansion of resources dedicated to addressing increasingly complex financial crime risks.

Looking ahead, staffing projections remain largely positive. While 57 percent of programs expect to maintain current staffing levels, another 42 percent anticipate growth — particularly among larger organizations. Only a single company foresees any decline, and none expects a significant reduction.

Taken together, these patterns indicate a sustained commitment across the industry to invest in talent and expertise, reinforcing the view that effectively combating financial crime requires continued — and in many cases increasing — staffing support (see Figure 7).

Figure 7 — Past and Future Staffing Trends



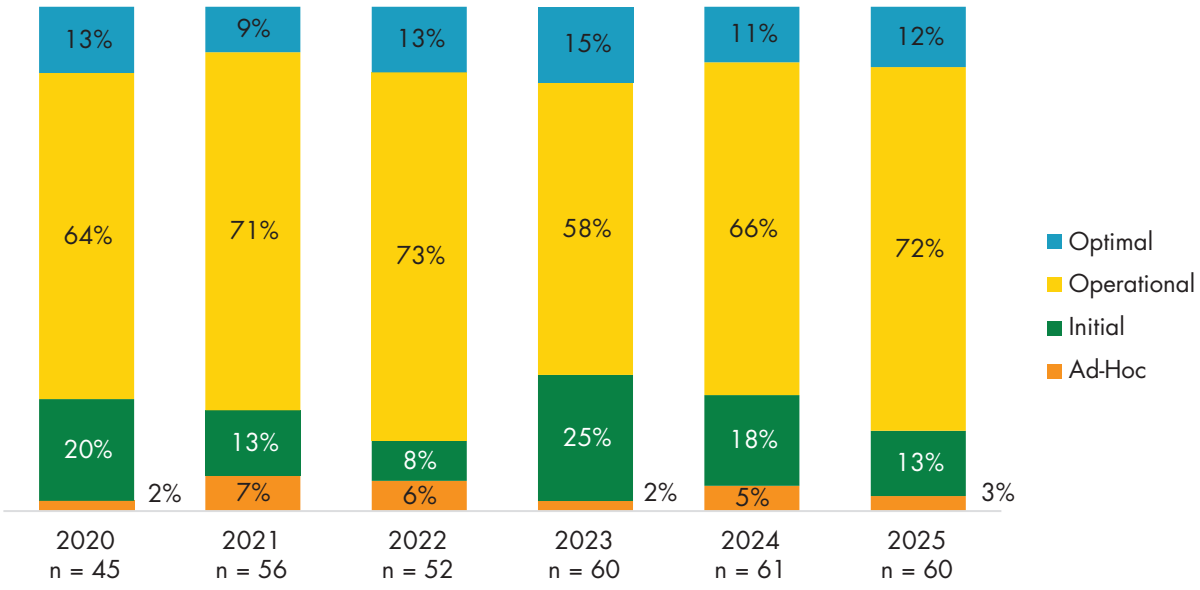
Note: Due to rounding, percentages may not total 100.

Program Maturity

For the past six years, most companies have categorized the maturity of their financial crimes and fraud prevention programs as "operational," reflecting a coordinated approach supported by documented policies and procedures. This year, 72 percent of companies fall into this category, while 12 percent consider their programs "optimal," characterized by defined governance structures, established risk assessment processes, and a commitment to continuous improvement (see Figure 8).

This distribution suggests that although many organizations have built solid, functional programs, relatively few have advanced to a stage where capabilities are fully mature and proactively evolving — highlighting continued opportunities for investment, refinement, and long term program development.

Figure 8 — Program Maturity



Note: Due to rounding, percentages may not total 100.

In 2025, 57 percent of companies believe their programs are on par with their peers. Additionally, 27 percent view their programs as slightly or very advanced, while 15 percent feel they are somewhat behind. This distribution highlights a generally confident industry posture, yet also suggests that a meaningful portion of organizations recognize the need to further enhance their capabilities to keep pace with evolving threats and leading practice expectations.

Strategic Insight:

Most life insurance and retirement services organizations have reached an **operational level of fraud program maturity**, with coordinated processes and documented controls in place, but relatively few have advanced to fully optimized, continuously evolving programs. While overall confidence is strong — most firms view their capabilities as on par with or ahead of peers — a meaningful segment recognizes gaps that could limit effectiveness as fraud risks become more complex and dynamic.

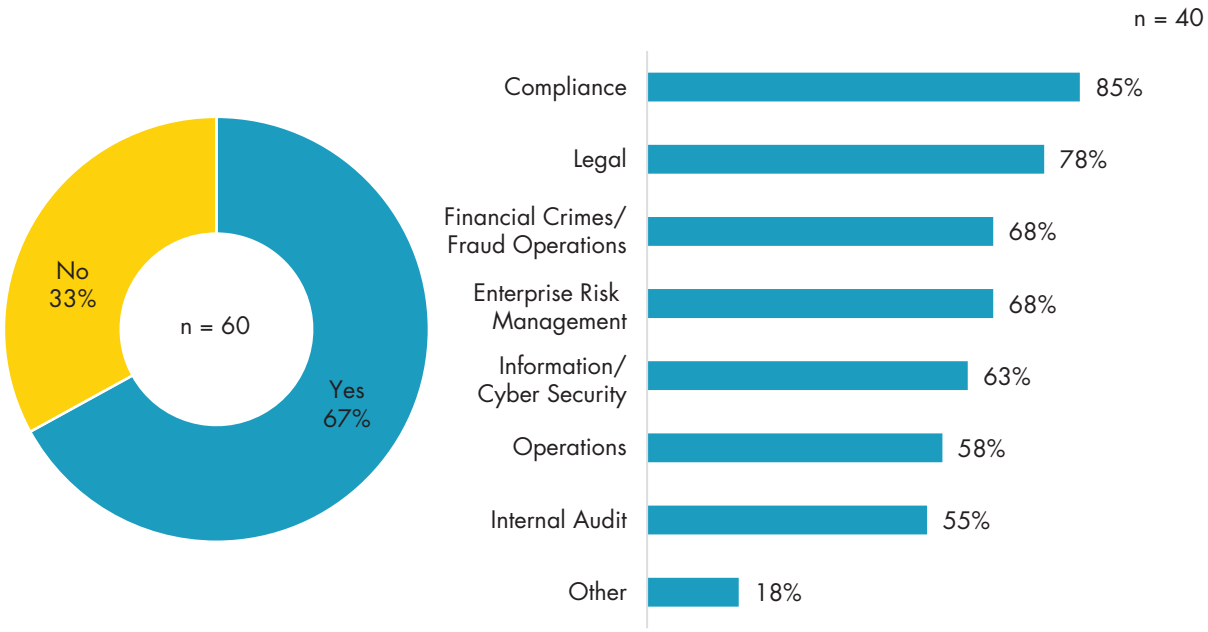
This maturity distribution highlights a strategic opportunity to move beyond baseline operational effectiveness toward **proactive, intelligence driven programs** that anticipate emerging threats and align with leading practices.

Governance and Reporting

Effective governance is essential to the success of financial crimes and fraud management programs. In 2025, 67 percent of companies have formal oversight committees or groups responsible for monitoring and guiding these programs — a practice especially common among organizations with more than 5,000 employees. These committees typically draw representation from three core areas: Compliance (85 percent), Legal (78 percent), and a third function such as Financial Crimes/Fraud Operations and Enterprise Risk Management (both at 68 percent).

This governance structure reinforces the importance of cross functional alignment and ensures that fraud prevention decisions are informed by legal, regulatory, operational, and risk management expertise. As threats become more complex, the presence of these oversight bodies positions companies to make faster, more coordinated decisions and maintain strong enterprise level accountability (see Figure 9).

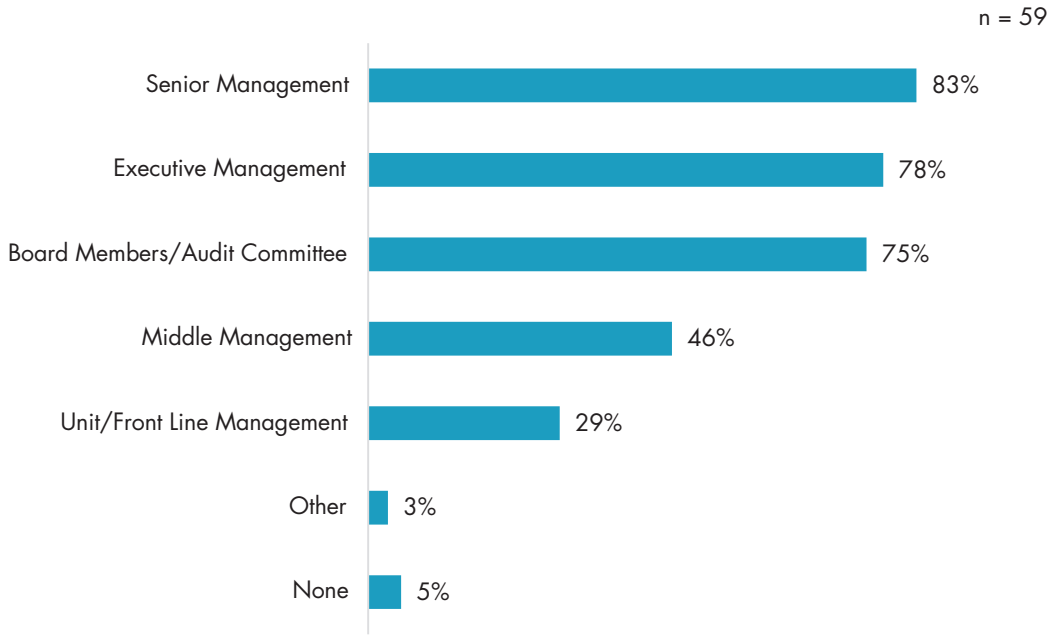
Figure 9 — Formal Oversight Committee or Group



Companies largely maintain strong upward reporting on financial crime and fraud, with most providing regular updates to senior management (83 percent), executive leadership (78 percent), and board members or audit committees (approximately 75 percent). This concentration of reporting at the highest levels reflects a clear emphasis on governance and oversight (see Figure 10).

In contrast, reporting diminishes significantly at lower organizational levels. Fewer than half of companies report regularly to middle management (46 percent), and fewer than one third extend reporting to unit-level or frontline management (29 percent), where emerging risks often surface first. While a small minority of organizations (5 percent) report providing no regular reporting, this likely reflects differences in organizational structure or program scale rather than a governance gap. Overall, the distribution underscores that fraud oversight is primarily treated as a strategic, enterprise-level responsibility, though the sharp drop-off at the front line may represent a potential blind spot where emerging issues often surface first.

Figure 10 — Regular Management Reporting



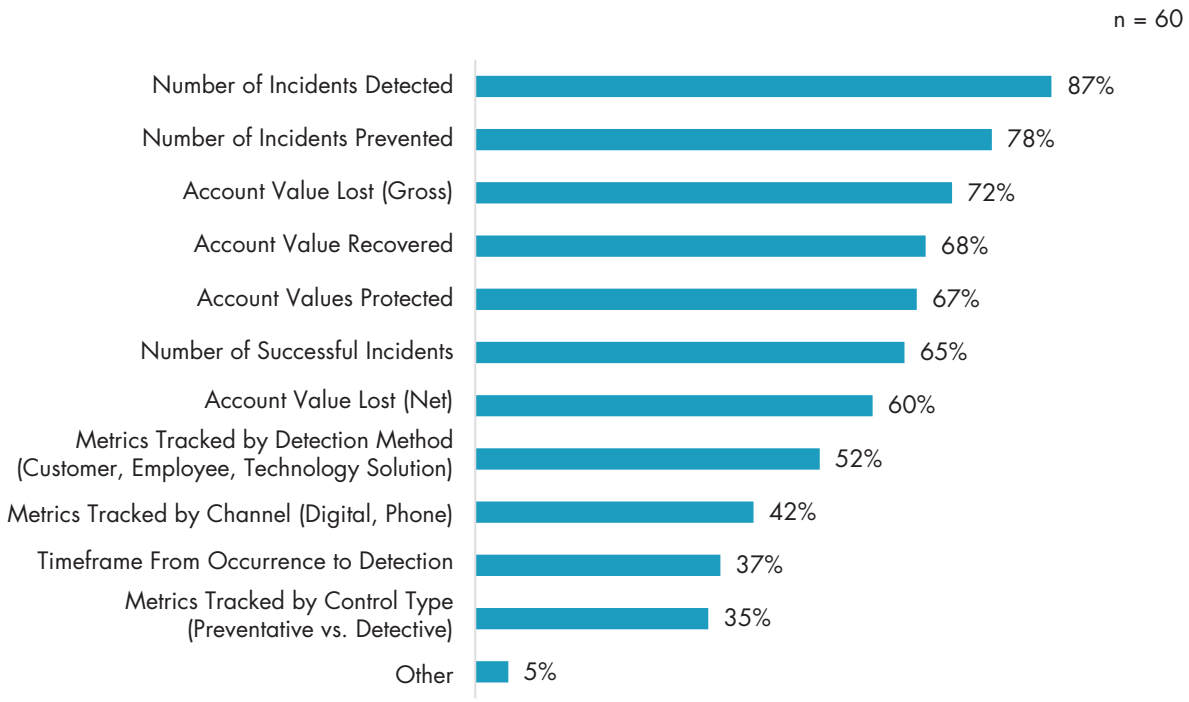
Strategic Insight:

Effective governance has become a defining strength for life insurance and retirement services companies, with most organizations establishing formal oversight committees and maintaining regular reporting to senior leadership and boards. This structure supports strong enterprise level accountability and enables more coordinated, informed decision making as financial crime and fraud risks grow in complexity.

However, the sharp drop off in reporting to middle and frontline management suggests a strategic opportunity to strengthen downward communication, ensuring emerging risks are identified and escalated earlier across the organization.

Companies use a wide range of metrics to assess the effectiveness of their financial crimes and fraud prevention programs. While the types of metrics have remained largely consistent over the years, the number of metrics used has steadily increased — rising by roughly one additional metric per year since 2021. In 2025, organizations are using an average of seven out of 12 available measures to evaluate program success. The most commonly used indicators continue to be those tied to the number of incidents detected or prevented (see Figure 11).

Figure 11 — Metrics of Success of the Program



Strategic Insight:

Life insurance and retirement services companies are steadily expanding how they measure fraud program effectiveness, signaling a shift toward more **data informed oversight and accountability**.

However, the continued emphasis on incident based metrics suggests an opportunity to evolve toward **forward looking and outcome driven measures** that better reflect prevention strength, customer impact, and long term risk reduction.

Reporting Among Peers

There is broad agreement among carriers on the value of sharing fraud metrics and control performance, with 93 percent of respondents acknowledging clear benefits. Consistent with last year's findings, most organizations that see value in this practice point to its role in strengthening internal processes by providing visibility into broader industry metrics and trends (91 percent). Respondents also emphasize the importance of leveraging insight into emerging threats affecting peers to justify new controls and investment decisions (89 percent).

Beyond internal improvements, many carriers view information sharing as a means of strengthening collective defenses. Four in 5 respondents note that sharing metrics helps build a more resilient industry overall (80 percent) and supports more informed discussions with senior leadership by providing context on peer performance and fraud prevention enhancements (80 percent). Taken together, this strong consensus highlights the critical role that transparency and collaboration play in advancing fraud prevention strategies across the industry.

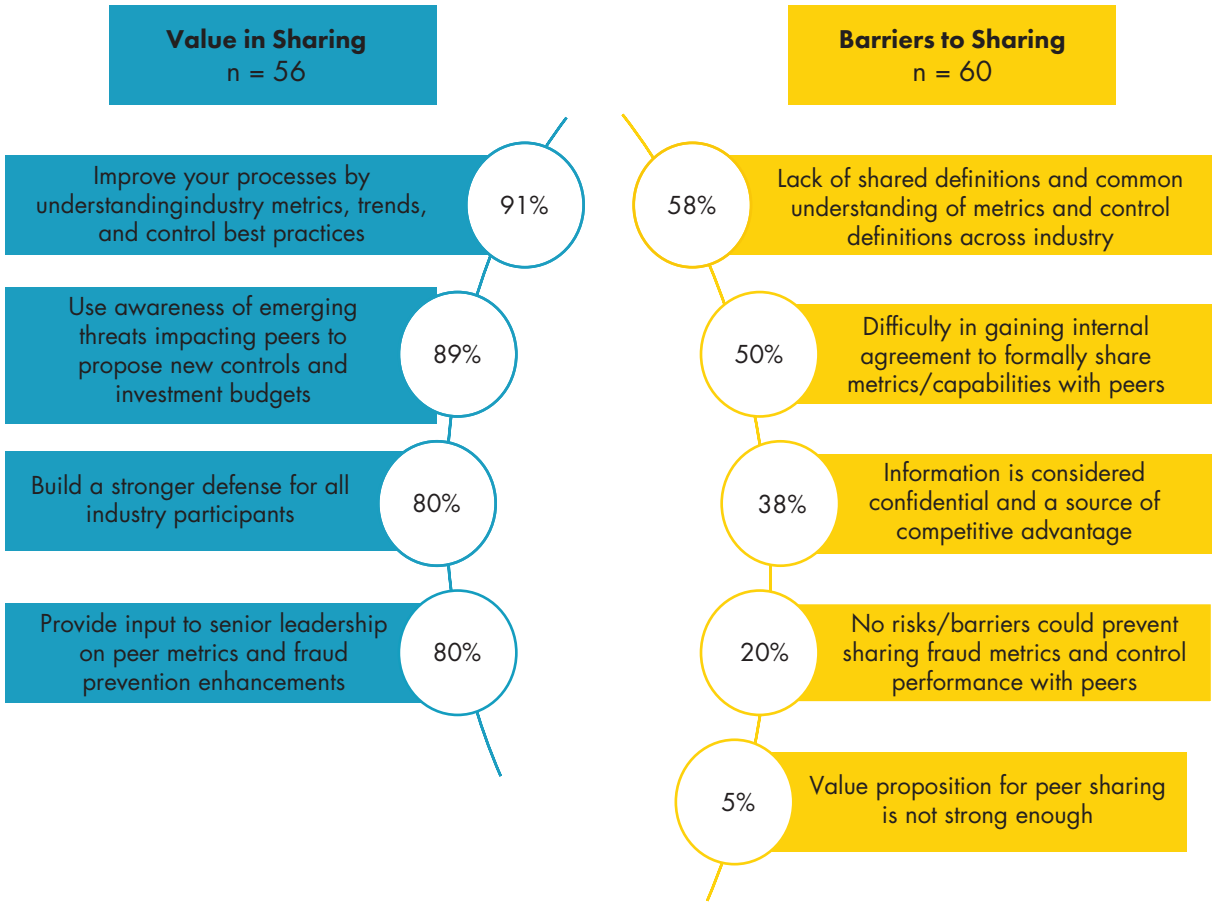
However, several factors continue to hinder broader data sharing. The most significant barrier — reported by 58 percent of respondents — is the lack of shared definitions and a consistent understanding of metrics and control terminology across companies (see Figure 12), while an additional 50 percent cite difficulty in gaining internal agreement to formally share metrics and capabilities with peers, underscoring that organizational alignment is nearly as challenging as external standardization. Addressing these challenges will require industry wide coordination to establish common standards, build trust among participants, and clearly demonstrate the operational value of shared insights; notably, 20 percent of respondents report seeing no risks or barriers to sharing metrics, suggesting that some organizations may already have the governance maturity or cultural readiness to participate more fully in collaborative data sharing efforts.

Strategic Insight:

Life insurance and retirement services companies overwhelmingly recognize that sharing fraud metrics and control performance strengthens both internal decision-making and collective industry defenses, particularly by improving visibility into peer trends and emerging threats.

However, inconsistent definitions and internal alignment challenges remain key barriers, signaling that greater industry standardization and governance maturity are critical to fully realizing the strategic value of collaborative data sharing.

Figure 12 — Value Versus Barriers in Sharing Fraud Metrics and Control Performance With Peers

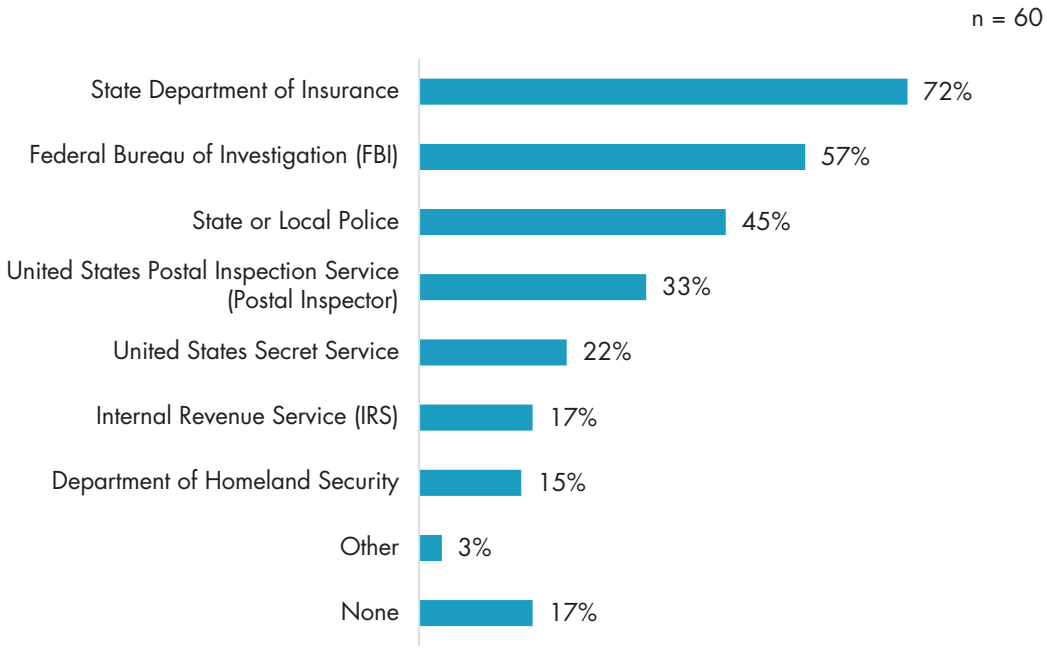


Law Enforcement and Reporting

Over the years, companies have consistently maintained standing relationships with an average of two to three law enforcement or government agencies, enabling them to tap into a wide range of resources, expertise, and investigative support. The most common partnerships are with State Departments of Insurance and the Federal Bureau of Investigation (FBI), reflecting the agencies most closely aligned with industry regulatory and enforcement needs.

Seventeen percent of companies, however, report having no standing relationships with law enforcement or government agencies. In some cases, this may reflect their unique circumstances — such as operating outside U.S. jurisdictions or no longer selling certain products — rather than a lack of interest or capability. Nonetheless, the absence of these relationships may limit access to timely information and coordinated support when fraud cases arise, potentially affecting the effectiveness of their overall fraud prevention efforts (see Figure 13).

Figure 13 — Standing Relationships With Law Enforcement/Government Agencies



Companies across the industry report fraud related information through a variety of regulatory and investigative channels. Nearly all organizations (93 percent) submit mandatory reports to state insurance departments, and more than half (54 percent) also engage in discretionary reporting. Additionally, 85 percent file Suspicious Activity Reports (SARs) with the Financial Crimes Enforcement Network (FinCEN), while 46 percent submit cases to the Internet Crime Complaint Center (IC3).

This multi-layered reporting framework demonstrates the industry's strong commitment to regulatory compliance and collaboration with enforcement bodies. By maintaining robust and diverse reporting practices, companies strengthen their ability to detect, document, and respond to emerging fraud risks — ultimately enhancing protections for both the organization and its customers.

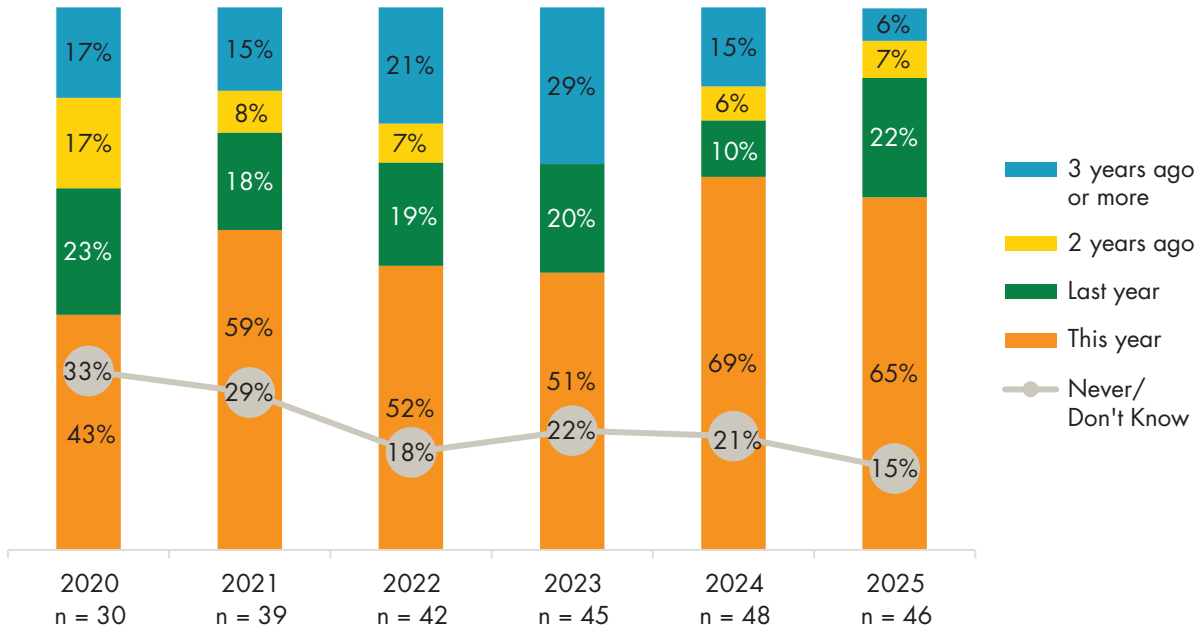
Fraud Risk Assessment

Formal fraud risk assessments are essential to building effective and efficient financial crimes and fraud prevention programs. They help companies understand their exposure to various risks and ensure that appropriate controls are in place. In practice, 44 percent of companies conduct these assessments annually, while another 20 percent complete them every other year (10 percent) or every third year (10 percent). Fifteen percent have never conducted a formal risk assessment — though in some cases this may reflect organizational circumstances, such as business model, jurisdiction, or program scope, rather than a lack of prioritization.

In the current landscape, 65 percent of companies completed their most recent assessment in 2025, reflecting a growing commitment to regularly evaluating financial crime and fraud vulnerabilities. Among those that have conducted assessments, 79 percent updated their programs as a direct result, demonstrating a proactive approach to adapting controls in response to emerging risks (see Figure 14).

While this overall progress signals increasing maturity across the industry, the fact that a portion of companies have not conducted a formal assessment suggests that practices vary and may be influenced by differing regulatory requirements or operational needs. Organizations without a formal process may still benefit from exploring alternative methods for evaluating risk exposure to ensure they remain aligned with evolving threats.

Figure 14 — Last Formal Risk Assessment Over the Years



Strategic Insight:

Organizations are making measurable progress in strengthening fraud and financial crime risk management through more frequent risk assessments, clearer program updates, and expanded insurance coverage, signaling growing maturity across the industry.

However, the lack of formal risk appetites for nearly half of companies — and gaps in insurance coverage for a minority — highlight uneven readiness, underscoring the need for clearer risk tolerances and more comprehensive protection as fraud and cyber threats continue to intensify.

Defined-risk appetites help ensure that limited resources are allocated efficiently, yet nearly half of companies (46 percent) still do not have a formal-risk appetite in place. Among the organizations that do, 22 percent base their risk appetite solely on financial thresholds, 6 percent focus only on reputational considerations, and 72 percent incorporate both. Consistent with the past six years, risk management departments continue to play a central role in setting risk appetite, with 63 percent of companies involving them in the process. Other functions — such as compliance (50 percent), executives (41 percent), and operations (31 percent) — remain active contributors.

Most companies mitigate their risk exposure by purchasing one or more types of insurance coverage, a practice that has steadily increased over time. Cybersecurity incidents and data breaches represent the most commonly insured risks, with 82 percent and 75 percent of companies, respectively, carrying commercial insurance for these events. However, 11 percent of companies report having no commercial insurance for fraud or cyber incidents, even as threats continue to escalate.

Together, these findings suggest that while many organizations are strengthening formal risk management practices and expanding insurance coverage, gaps remain. The absence of defined risk appetites in nearly half the industry, combined with some companies lacking key insurance protections, indicates uneven readiness. As fraud and cyber threats intensify, organizations without clear risk tolerances or adequate coverage may face greater exposure and fewer safeguards when incidents occur.

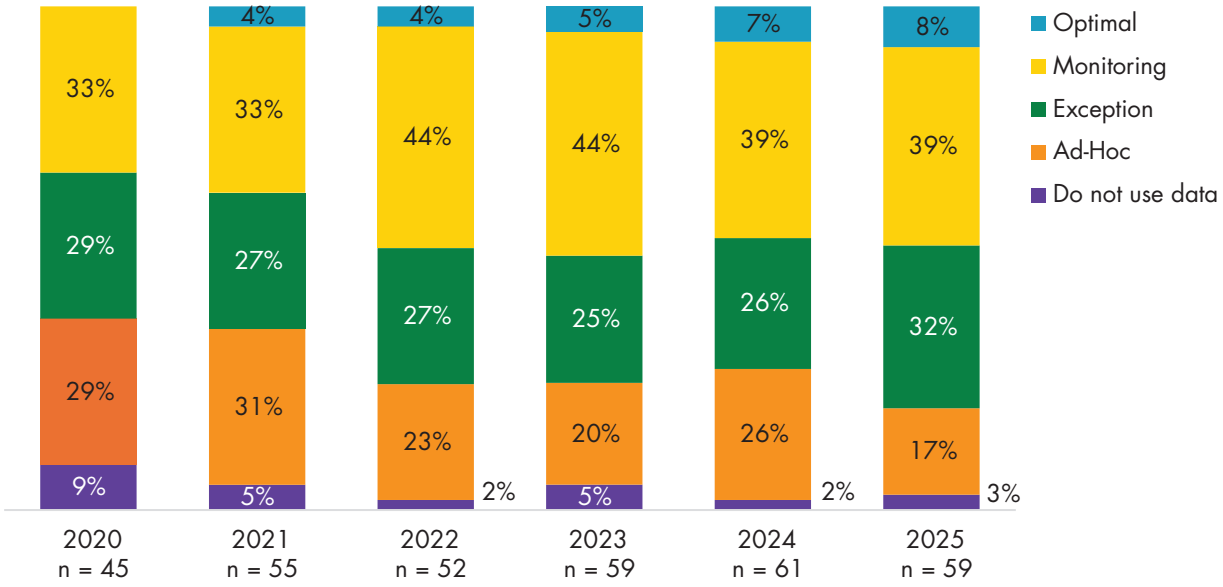
Technology and Spending

Technology

Companies vary widely in how they use data to support proactive fraud detection and prevention. The largest share (39 percent) operate at the monitoring stage, where alerts are generated through trend and pattern analysis to identify unusual interactions or transactions. Company size plays a significant role in determining the maturity of these practices: organizations with fewer than 500 employees are more likely to be at the ad hoc- or exception based stages, while companies with more than 5,000 employees tend to operate at the monitoring or optimal level, reflecting the advantages that scale brings in terms of tools, talent, and analytic sophistication. Notably, only 3 percent of companies report not using data proactively — an improvement from 9 percent in 2020 (see Figure 15).

These differences underscore a broader implication: as fraud schemes become more complex and data driven, companies with less mature analytics frameworks — often smaller organizations — may face greater challenges in detecting threats early. Meanwhile, the steady decline in companies not using data at all signals an industry gradually moving toward more advanced, proactive detection capabilities.

Figure 15 — Maturity of Use of Data in Fraud Detection and Prevention



Data Accessibility

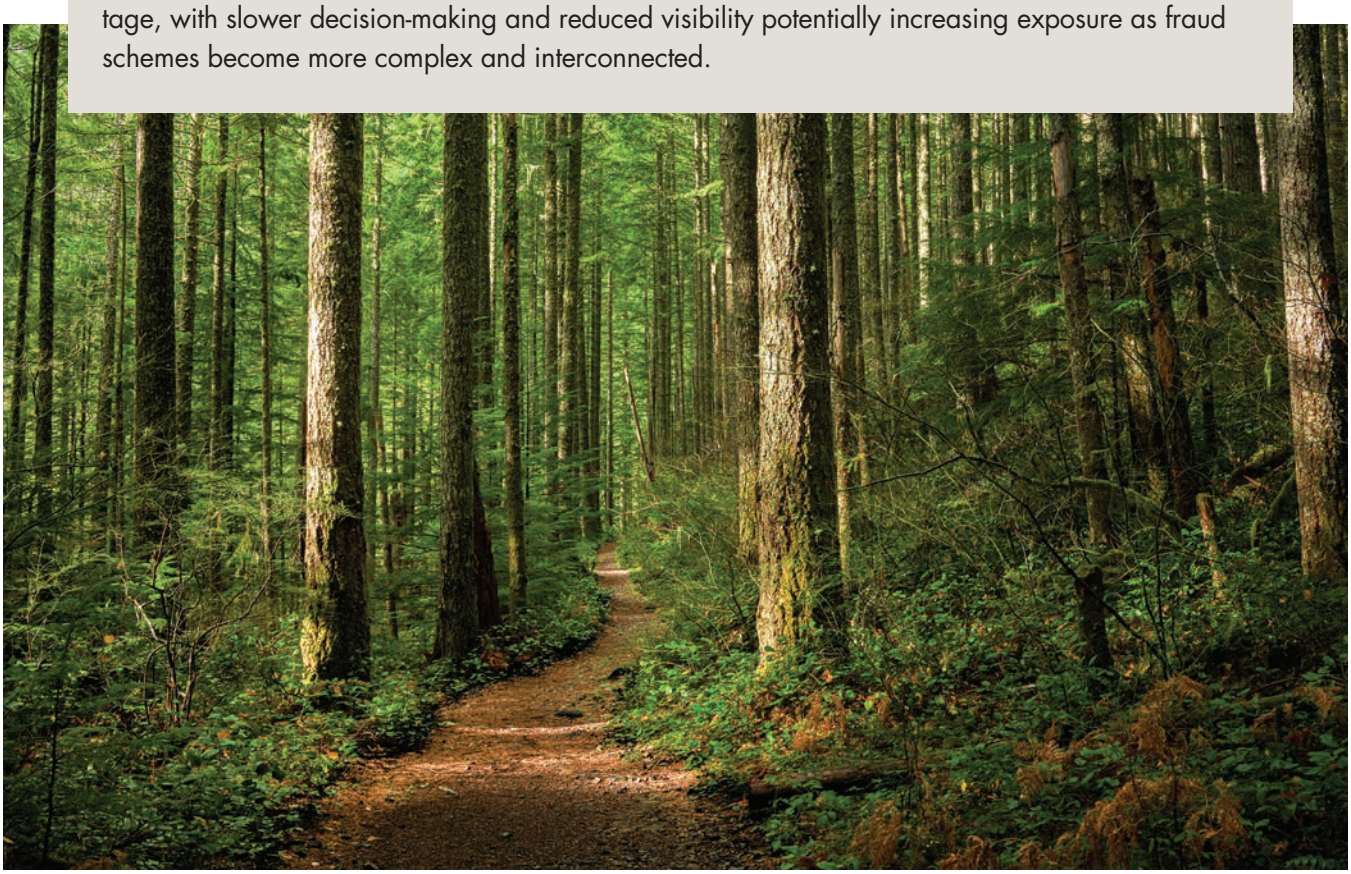
Most insurance companies have made substantial progress in aggregating key data sources, with 80 percent achieving centralized customer data, 75 percent aggregating account data, and 73 percent doing so for transaction data. This continued movement toward centralized data environments strengthens companies' ability to manage information consistently and apply more advanced analytics to detect emerging fraud patterns.

However, 8 percent of companies still lack aggregated views across these datasets, which limits their ability to generate comprehensive insights and respond quickly to complex fraud schemes. As the industry increasingly shifts toward integrated data solutions, organizations without unified data structures may face growing gaps in analytical capability, decision making speed, and operational efficiency — potentially leaving them more vulnerable as fraud threats evolve.

Strategic Insight:

Most insurance companies have built strong foundations through centralized customer, account, and transaction data, enabling more consistent information management and advanced fraud analytics.

However, organizations without fully integrated data environments remain at a strategic disadvantage, with slower decision-making and reduced visibility potentially increasing exposure as fraud schemes become more complex and interconnected.



Tools

Companies use a broad range of tools to authenticate customers and identify and investigate fraudulent activity, drawing from a landscape of 45 available solutions (see Table 1 for the top 10). The most widely used tools include LexisNexis Accurint (80 percent), FraudShare (77 percent), and Refinitiv GIACT (53 percent). In addition, 37 percent of companies report relying on tools developed in house, underscoring the continued need for customized solutions.

On average, companies use eight tools, though adoption varies significantly by size. Larger organizations (5,000+ employees) typically deploy closer to 11 tools, while smaller companies (<500 employees) rely on about four. This variation illustrates how scale influences the sophistication and layering of fraud prevention defenses. Larger organizations often require multiple point solutions to address diverse risks across product lines and channels, while smaller companies may lean on fewer tools due to resource constraints or simpler operational structures.

Companies are also exploring new capabilities, with organizations considering an average of two additional tools or services. Interest is strongest in Pindrop Passport (17 percent), Pindrop Protect (14 percent), and Socure (12 percent). However, 41 percent of companies are not considering any new tools, suggesting that many believe their current toolsets are adequate — or that integration challenges, budget limitations, or overlapping functionality limit the appetite for expansion.

Taken together, these adoption patterns indicate that while the industry continues to diversify its fraud prevention technology stack, growth in new tool deployment may be slowing as companies focus on optimizing what they already use. As fraud schemes evolve, organizations that rely on fewer tools or delay modernization may face increasing pressure to reassess whether their current capabilities are sufficient to keep pace.

Table 1 — Top 10 Tools or Services to Help Authenticate, Identify, and Investigate Fraudulent Activity

	Companies Using n = 60
1. LexisNexis Accurint	80%
2. FraudShare	77%
3. Refinitiv GIACT	53%
4. Evadata Act	38%
5. Tools Developed In-House	37%
6. LexisNexis Instant ID QA	37%
7. TransUnion TLO	35%
8. FS-ISAC	32%
9. Splunk	30%
10. Pindrop Protect	28%

Companies rely on a range of case management tools to track and monitor suspicious activity referrals (see Table 2 for the top five). In house tools remain the most commonly used solution, adopted by 33 percent of companies, followed by widely used platforms such as Salesforce, Archer, ServiceNow, and Actimize. Although usage patterns have shifted somewhat over the years, inhouse tools have consistently remained a popular choice — likely due to their flexibility, customization potential, and alignment with internal workflows.

Notably, 10 percent of companies reported not using any case management system in 2025. On average, companies use two types of tools, while larger organizations (5,000+ employees) tend to use closer to three. This difference reflects both the complexity of larger operations and the need for layered systems capable of handling higher volumes, broader reporting requirements, and more sophisticated investigative processes.

When looking at future adoption, 67 percent of companies are not considering adding new case management tools, while 12 percent are planning to develop new in house capabilities. On average, companies are exploring just one additional solution.

These trends imply that many organizations may be shifting from expansion to optimization — focusing on improving the efficiency, integration, or configurability of existing systems rather than layering on new technology. However, the absence of any case management system among a subset of companies highlights potential vulnerabilities, as lacking structured case tracking can hinder documentation, oversight, and the ability to identify emerging patterns.

Table 2 — Top Five Case Management Tools to Track and Monitor Suspicious Activity Referrals

	Companies Using n = 60
1. Tools Developed In-House	33%
2. SalesForce	13%
3. Archer	12%
4. Service Now	12%
5. Actimize	10%
6. None	10%

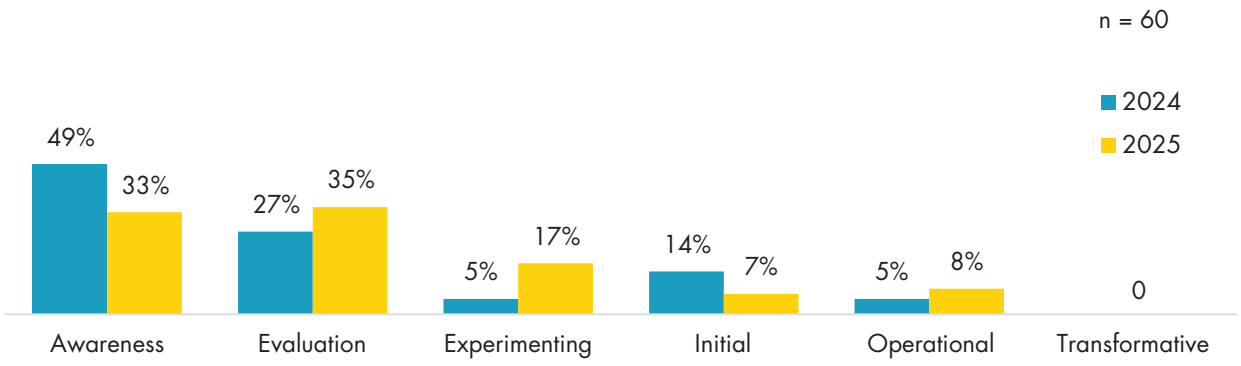
AI Technology

When asked about their maturity in using AI to enhance fraud-prevention capabilities, companies showed a notable shift along the maturity scale in 2025. Only 33 percent of organizations remain at the awareness stage — down from 49 percent in 2024 — indicating that fewer companies are merely aware of AI's potential without yet evaluating or adopting it (see Figure 16). This year, 35 percent have progressed to the evaluation stage, actively assessing AI tools, while 17 percent are at the experimenting stage, where AI capabilities are being tested but not yet deployed in production.

A smaller share has moved into the initial or operational stages, and no companies have reached the transformative stage, where multiple AI use cases generate meaningful, measurable results across the program.

These shifts imply that while the industry is slowly advancing its AI maturity, most organizations are still in the early phases — focused on understanding, assessing, or piloting AI rather than deploying it at scale. The lack of companies in the transformative stage suggests that operationalizing AI for fraud prevention remains a significant challenge, likely due to factors such as data quality, model governance, integration complexity, and organizational readiness. As threats grow more sophisticated, companies that remain in early stages may face increasing pressure to accelerate adoption to keep pace with AI driven fraud techniques.

Figure 16 — Maturity in Using AI to Enhance Fraud Prevention Capabilities



On average, companies identified three barriers to implementing AI for fraud prevention. The most significant challenges (see Figure 17) include limited availability of internal resources (62 percent), data quality or data access issues (53 percent), and a lack of internal expertise (47 percent). Together, these barriers indicate that many organizations are still struggling with the foundational elements required for effective AI adoption.

The high rate of resource related concerns suggests that companies often lack the personnel capacity or dedicated time needed to evaluate, pilot, and operationalize AI tools. Data quality and access issues — especially prevalent among larger companies (76 percent) — underscore that without clean, well structured, and accessible data, AI models cannot perform reliably, limiting their value. Meanwhile, the shortage of internal expertise highlights a growing skills gap in areas such as data science, AI model governance, and fraud analytics.

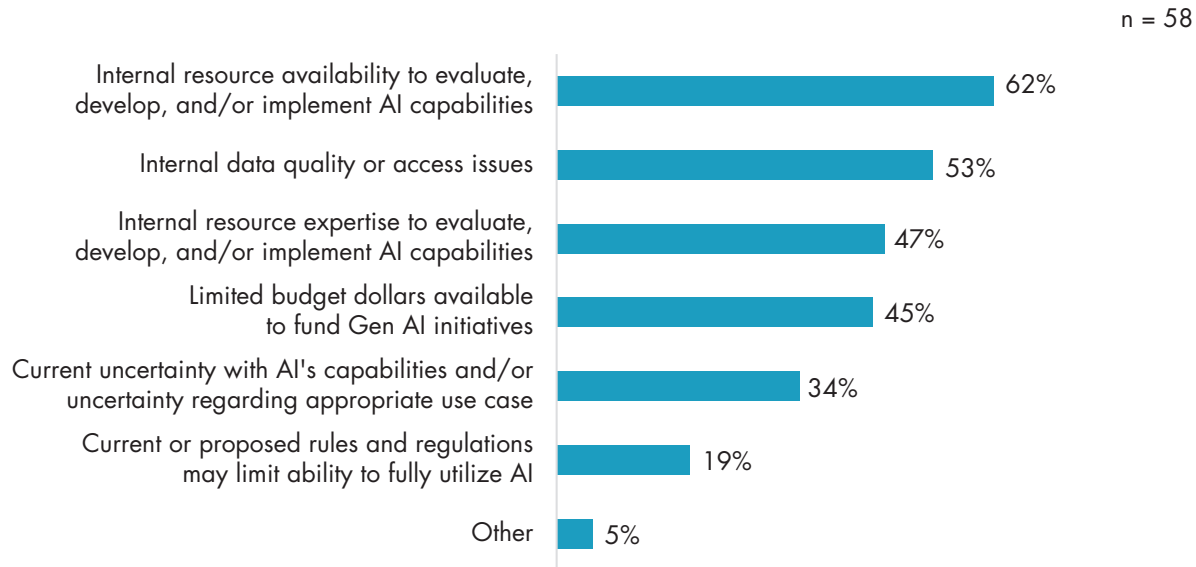
These barriers collectively imply that while interest in AI-enabled fraud prevention is growing, many organizations are not yet structurally or technically ready to adopt AI at scale. Addressing these foundational gaps will be essential for companies aiming to move beyond early experimentation and fully leverage AI to enhance fraud detection and response.

Strategic Insight:

The insurance industry is steadily advancing its AI maturity for fraud prevention, with fewer organizations remaining in the awareness phase and more actively evaluating or experimenting with AI capabilities. However, the absence of companies in the transformative stage underscores that AI adoption remains largely nascent, constrained by foundational challenges such as resource limitations, data quality issues, and skills gaps.

As fraud threats become increasingly AI-driven, insurers that fail to accelerate beyond pilot efforts risk falling behind more prepared peers who can operationalize AI at scale.

Figure 17 — Barriers to Implementing Fraud Prevention Capabilities Utilizing AI



Spending

While most companies report relatively consistent year over year spending, this year 63 percent indicated their budgets remained about the same as the previous year, while 37 percent reported an increase compared to 2024. Looking ahead to 2026, 60 percent of companies expect to maintain current spending levels, and 40 percent anticipate increasing their budgets. Notably, 89 percent of smaller companies plan to spend the same amount next year. No companies reported spending less than last year, nor do any plan to reduce spending in the coming year — reinforcing the industry's sustained commitment to addressing rising fraud threats.

With respect to anticipated expenditure levels, 46 percent of companies project investing less than $250,000 in fraud prevention and authentication technologies (excluding cybersecurity) over the next year. A further 32 percent expect to allocate between $250,000 and $1 million, while 22 percent anticipate spending in excess of $1 million.

These patterns imply that fraud prevention spending is stabilizing at higher levels rather than expanding indefinitely. Companies appear to be moving from rapid budget growth toward steady, ongoing investment — suggesting that fraud prevention is becoming a core operational cost rather than a discretionary one. At the same time, the sharp contrast between smaller companies holding budgets flat and larger companies increasing spending highlights a widening capability gap. As fraud schemes grow more sophisticated, organizations with limited budget flexibility may find it increasingly difficult to keep pace with evolving threats and technology demands.

AI Spending

In 2025, 59 percent of companies plan to invest in AI-driven fraud prevention initiatives, representing a substantial increase from 34 percent in 2024. Among organizations planning to invest, 74 percent expect to increase their AI-related spending relative to current levels, while none anticipates a reduction. The remaining 26 percent expect spending to remain unchanged. Investment momentum is strongest among larger organizations, with 71 percent of companies employing more than 2,000 people planning to invest in AI next year, compared with 44 percent of smaller firms — underscoring the role of organizational scale in enabling investment in advanced technologies.

However, the relative weight of these AI investments varies considerably. For 59 percent of companies, planned AI spending for 2026 does not represent a meaningful share of their total budget for new initiatives. Only 41 percent view their AI fraud prevention investment as a significant portion of overall new initiative spending. Smaller companies are more likely to see their AI spend as meaningful (50 percent) compared with larger organizations (33 percent), suggesting that even modest investments represent a larger strategic commitment for them.

These trends imply that while adoption of AI in fraud prevention is accelerating, many companies are still treating AI as an incremental enhancement rather than a major investment priority. Larger organizations may be spreading resources across multiple innovation efforts, whereas smaller firms — though less likely to invest — tend to feel the impact of these investments more acutely. As AI-enabled fraud threats grow more sophisticated, the companies treating AI as a secondary spend may find themselves pressured to elevate its priority to keep pace with emerging risks.

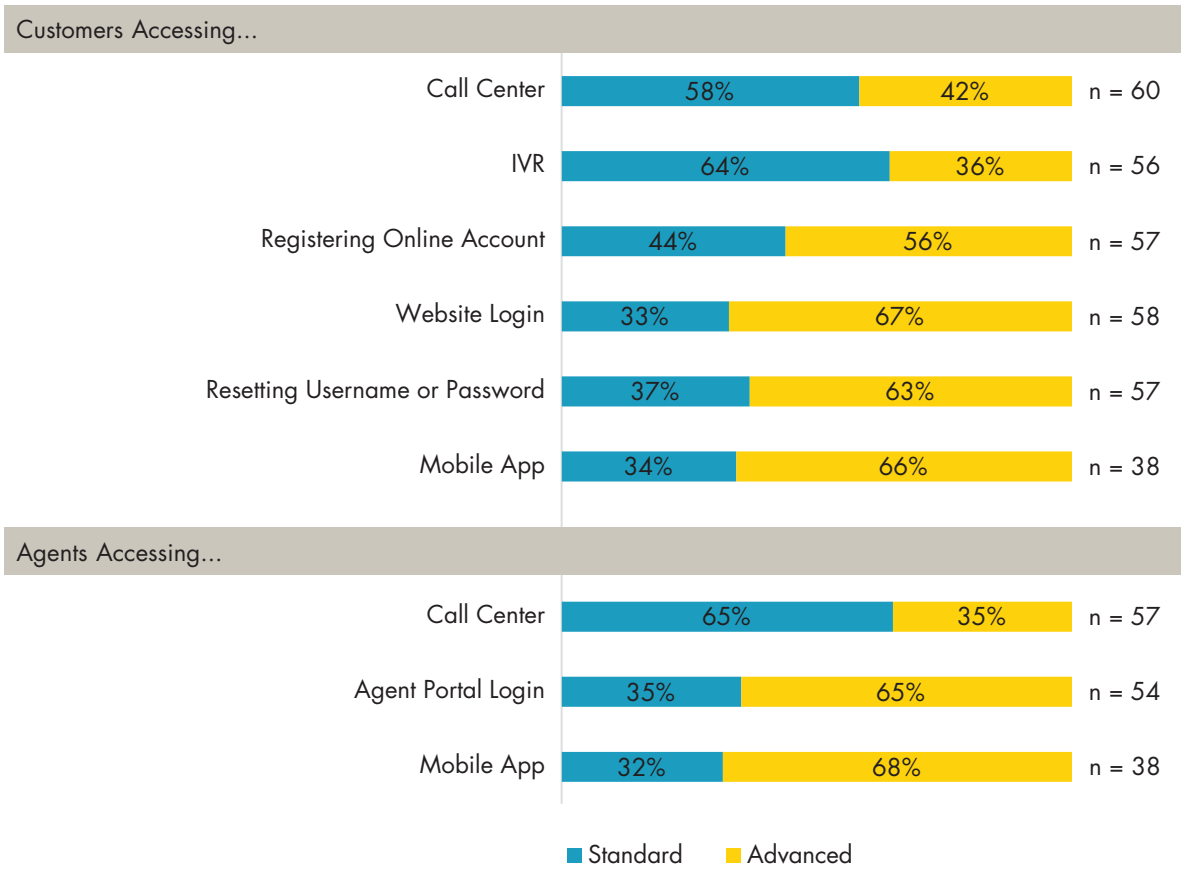
Authentication

Many organizations continue to rely primarily on standard customer identifiers — such as name, Social Security number (SSN), date of birth, and contract number — to authenticate customers and agents across channels (see Figure 18). In call centers, 58 percent of companies depend mainly on these basic identifiers, while 42 percent supplement them with advanced authentication. Reliance on standard identifiers is even higher in IVR systems, where 64 percent use basic methods and only 36 percent employ advanced authentication. Most companies apply enhanced authentication controls for high risk call center interactions, though coverage is stronger for customers than for agents. About 7 in 10 organizations use stepped up customer authentication for high risk transactions, transactions exceeding defined thresholds, or when suspicious activity is detected, while fewer — just under 6 in 10 — apply similar stepped up authentication procedures for agents under comparable risk conditions.

By contrast, digital channels demonstrate more mature practices: 66 percent of companies use advanced authentication for mobile app users, and 67 percent do so for website logins. Agent authentication follows a similar pattern. While 65 percent of organizations rely on standard methods to authenticate agents calling into contact centers, significantly fewer use standard methods for digital access — 35 percent for agent portals and 34 percent for mobile apps — indicating greater adoption of stronger controls in lower-friction, digital environments.

Overall, these patterns suggest that legacy reliance on basic identifiers remains a key vulnerability in voice-based channels, where fraud risk is highest, while digital channels benefit from more robust authentication investments.

Figure 18 — Level of Sophistication of Authentication for Different Kinds of Access



Companies employ a range of authentication methods to verify customers and agents across access channels, with one-time passcodes (OTPs) delivered to mobile phones or landlines remaining the most widely used approach. OTPs are especially prevalent in customer-facing interactions — including call centers, IVR systems, websites, account recovery, and mobile apps — as well as for agent authentication in call centers and agent portals.

Device identification is also commonly used, particularly in digital environments, reinforcing layered security for online and mobile access. At the same time, adoption of biometric authentication is increasing, especially for mobile access, where it has emerged as one of the leading authentication methods. Biometrics are also gaining traction in IVR environments, reflecting growing confidence in their ability to balance security with low user friction.

Overall, advanced authentication is more prevalent in digital channels than in voice-based interactions, suggesting that organizations are prioritizing stronger, lower-friction controls where implementation is more straightforward. For agents using mobile applications, the growing use of authenticator apps and device-based authentication signals a shift toward more resilient access controls for distributed and field-based workforces. These trends indicate progress toward stronger authentication, while highlighting continued exposure in voice channels that remain heavily dependent on legacy methods (see Table 3).

Table 3 — Top Three Authentication Methods for Different Kinds of Access

	The Top Three Authentication Methods		
	1st	2nd	3rd
Customers Accessing…			
Call Center **n = 25**	64% One-Time Passcode Sent to Cell or Land Line	48% One-Time Passcode Sent to Email	48% Knowledge-Based Questions Only When Other Risk Signals or Red Flags are Observed
IVR **n = 19**	53% One-Time Passcode Sent to Cell or Land Line	47% Device Identification	42% Voice Biometrics
Register Online Account **n = 31**	84% Phone Ownership Verification with One-Time Passcode	61% Email Confirmation with or without One-Time Passcode	39% Technology Enabled Anomaly Detection (Internally Developed or 3rd Party Utility) and Knowledge-Based Questions (tie)
Website Login **n = 37**	86% One-Time Passcode Sent to Cell or Land Line	76% One-Time Passcode Sent to Email	54% Device Identification
Resetting Username or Password **n = 36**	81% One-Time Passcode Sent to Cell or Land Line	61% One-Time Passcode Sent to Email	44% Knowledge-Based Questions
Mobile App **n = 21**	76% One-Time Passcode Sent to Cell or Land Line	52% Device Identification	43% Biometrics and One-Time Passcode Sent to Email (tie)
Agents Accessing…			
Call Center **n = 18**	50% One-Time Passcode Sent to Cell or Land Line	47% Knowledge-Based Questions for All Calls	35% One-Time Passcode Sent to Email
Portal Login **n = 35**	60% One-Time Passcode Sent to Cell or Land Line	50% Device Identification	38% One-Time Passcode Sent to Email and Authenticator App (Push Notification or OTP) (tie)
Mobile App **n = 20**	67% Authenticator App (Push Notification or OTP)	42% Device Identification	33% One-Time Passcode Sent to Cell or Land Line

Looking ahead, 37 percent of companies are not currently considering additional authentication tools. Among those are, organizations expect to add two new capabilities on average. Device identification is the most frequently considered option (24 percent), followed by voice biometrics and authentication apps (see Figure 19).

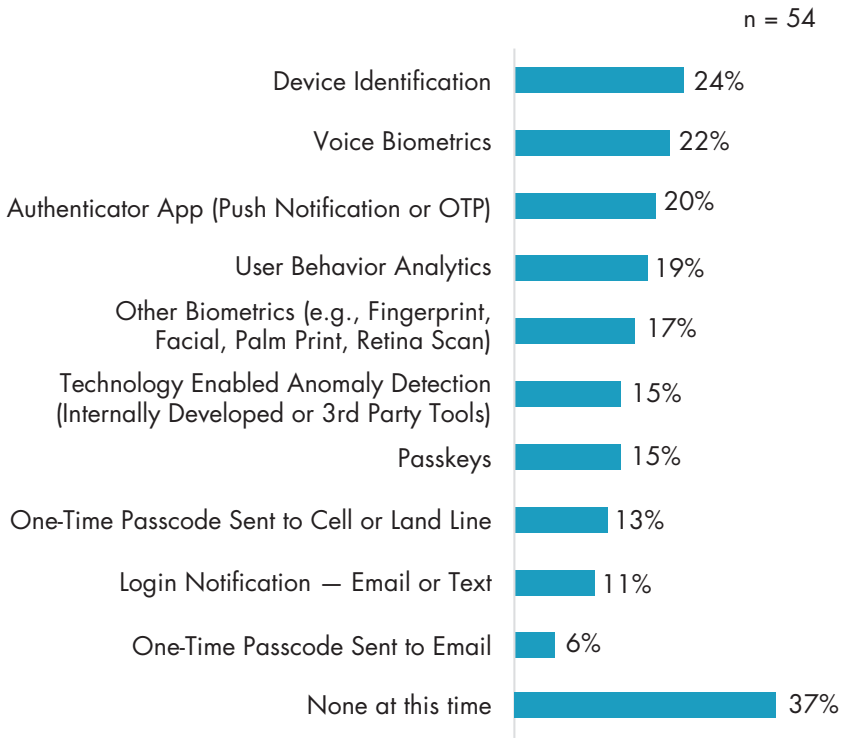
These trends suggest a gradual but steady shift toward multifactor authentication, indicating that companies increasingly recognize the need to supplement traditional identifiers with layered security measures to better protect against sophisticated fraud attempts.

Strategic Insight:

Most insurers have strengthened authentication in digital channels, but continued reliance on basic identifiers in voice-based interactions — where fraud risk is highest — remains a critical vulnerability. While stepped-up controls are commonly applied to high-risk customer transactions, inconsistent agent authentication and uneven use of advanced methods across channels limit overall effectiveness.

The gradual move toward multifactor authentication signals progress, but organizations that delay modernizing voice-channel controls risk exposure as impersonation and social-engineering attacks continue to escalate (see Figure 20).

Figure 19 — Advanced Authentication Capabilities Under Consideration



Transactions Enablement

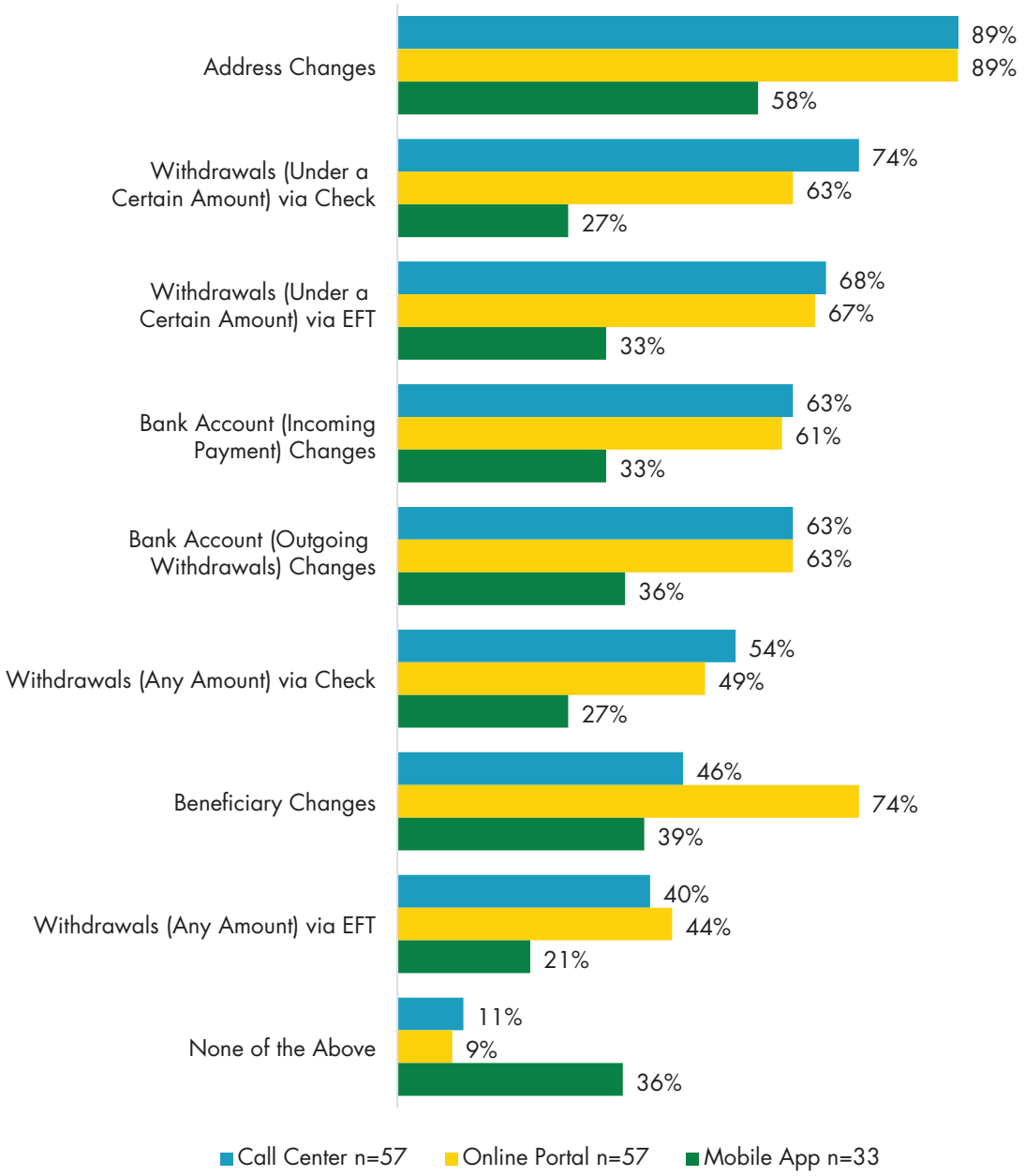
Companies continue to expand the range of transactions available across call centers and digital channels, though capabilities vary significantly by channel. Call centers support an average of five transaction types and remain the most comprehensive channel, enabling a wide range of activities including address changes, limited withdrawals by check or electronic funds transfer (EFT), and both incoming and outgoing bank account updates.

Online portals now match call centers in breadth, also supporting an average of five transaction types. The most commonly enabled online transactions include address changes, beneficiary updates, and limited withdrawals via EFT, reflecting growing customer self-service adoption for moderately complex activities.

Mobile apps, by contrast, remain more limited, typically supporting only two transaction types. While address and beneficiary changes are commonly available, higher-risk transactions such as withdrawals and bank account updates are far less prevalent. Notably, more than one third of mobile apps do not support any of the listed transactions, compared with a much smaller share of call centers and online portals.

These patterns suggest that organizations continue to prioritize transaction depth in call centers and web channels, while taking a more cautious approach to mobile functionality — likely due to security, authentication, and fraud risk considerations. As mobile usage continues to grow, the limited transaction support may represent both a risk-mitigation strategy and a missed opportunity to improve customer experience through secure expansion of mobile capabilities.

Figure 20 — Transaction Capabilities



Strategic Insight:

Organizations continue to concentrate higher-risk transactions in call centers and online portals, pairing expanded self-service capabilities with strong, consistently applied verification controls. By contrast, mobile channels remain intentionally constrained, with slower expansion plans and more variable verification practices — particularly for EFT withdrawals and bank account changes — reflecting heightened fraud concerns.

As digital usage grows, insurers that can align mobile transaction expansion with robust, consistent controls across channels will be best positioned to reduce risk while meeting rising customer expectations.

On average, companies plan to add two new online transaction capabilities over the next one to two years. Among those that do not currently offer specific transactions online, roughly 30 percent–40 percent expect to enable functions such as bank account changes for incoming payments (42 percent), withdrawals under a certain amount via check (36 percent), outgoing bank account changes (30 percent), and withdrawals under a certain amount via EFT (30 percent).

Expectations are notably lower for enabling withdrawals of any amount, with only about 14 percent anticipating future support via check or EFT. At the same time, 9 percent of companies do not expect to add any additional online transaction capabilities at all. For mobile apps, planned expansion is more limited: among companies that do not yet support these functions in their apps, only 17 percent–20 percent anticipate enabling any of the listed transactions, and 36 percent do not expect to expand mobile app transaction capabilities over the next one to two years.

Restrictions on withdrawals based on online and mobile transactions are common. For online transactions, companies apply strong and consistently enforced verification controls before processing withdrawals. Most organizations verify recent address changes prior to approving online withdrawals and impose a waiting period before disbursing funds following an address change. Bank account verification is similarly robust, with many companies confirming bank account ownership for all EFT withdrawal amounts and restricting disbursements after a bank account change (see Table 4).

Mobile app transactions, however, are governed by more variable verification practices. While many companies review recent address changes before processing withdrawals issued by check, controls weaken for mobile EFT withdrawals. Fewer companies confirm bank account ownership for all EFT amounts, and a meaningful share do not verify ownership at all before processing. In addition, most companies do not restrict disbursements following a bank account change for mobile withdrawals, despite improvement from prior years.

Table 4 — Digital Withdrawal Controls

	Online (n = 40-42)	Mobile App (n = 12-13)
Check for recent address changes before processing withdrawals through:	88%	75%
Restrict disbursements for a defined time period after address changes made:	73%	42%
Confirm bank account ownership prior to processing withdrawals via EFT through:	74% yes, all 19% yes, with threshold 7% no	54% yes, all 23% yes, with threshold 23% no
Restrict disbursements for a defined time period after address changes made:	50%	38%

Fraud Training and Awareness

For Company Affiliates

Nearly all companies (98 percent) require regular financial crimes and fraud awareness training for employees — a trend that has remained stable for six years and reflects broad industry recognition that employee education is a critical frontline defense. Requirements extend beyond employees, with 53 percent of companies mandating training for agents and field associates. Contractors are also frequently included: 62 percent of companies require training for this group, an important practice given the growing reliance on third party and contingent staff. Notably, every company surveyed reported having at least some form of required training in place, underscoring the universal view that fraud awareness education is nonnegotiable.

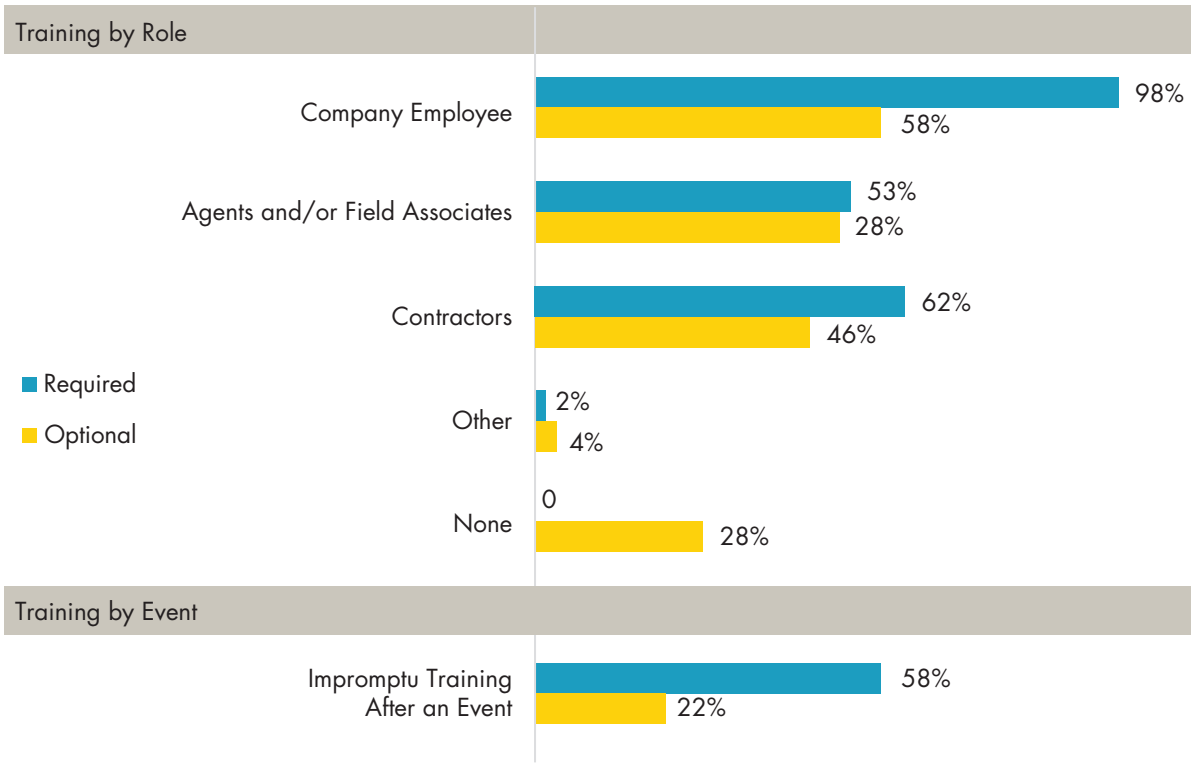
Optional training opportunities are also common. Fifty-eight percent of companies offer optional training for employees, and 51 percent do so for agents and field associates. Contractors are included in optional programs at 46 percent of companies. However, 28 percent of organizations offer no optional training at all, indicating a missed opportunity to reinforce awareness and deepen learning beyond baseline requirements.

In addition, 80 percent of companies provide impromptu training following a major fraud event to highlight scheme characteristics and red flags. Of these, 58 percent make such training mandatory — a proportion that has increased over time — while 22 percent offer it on an optional basis. Still, approximately 20 percent of companies do not provide any ad hoc training after significant incidents, suggesting a potential gap in their ability to quickly reinforce lessons learned and strengthen organizational readiness (see Figure 21).

Most organizations report that employees spend less than five hours per year on training (81 percent), and a similar percentage (87 percent) report that agents or agent support staff also spend fewer than five hours annually. This level of time investment has been consistent for the past six years and suggests that while companies maintain strong foundational training practices, there may be limits to how deeply staff can engage with evolving fraud risks.

Taken together, these patterns show that while required training is nearly universal, optional and event driven training practices vary widely. Companies that limit training to required minimums may miss opportunities to reinforce emerging fraud trends, especially as threats evolve rapidly and often exploit human vulnerability. The relatively low annual training hours further indicate that organizations may need to rethink how to deliver more impactful, continuous learning — especially for roles closest to customers or sensitive transactions. Strengthening both the depth and frequency of training could better position companies to stay ahead of new fraud schemes and reduce operational risk.

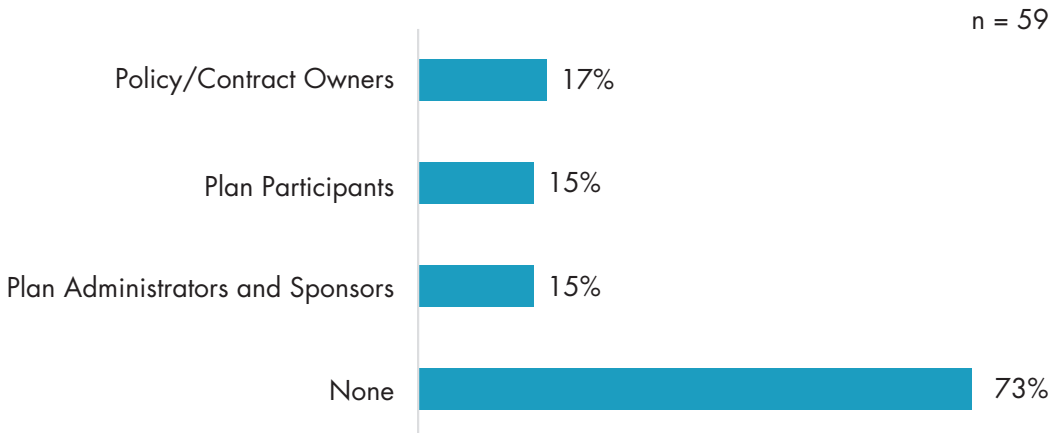
Figure 21 — Training by Role and by Event



For Customer Groups

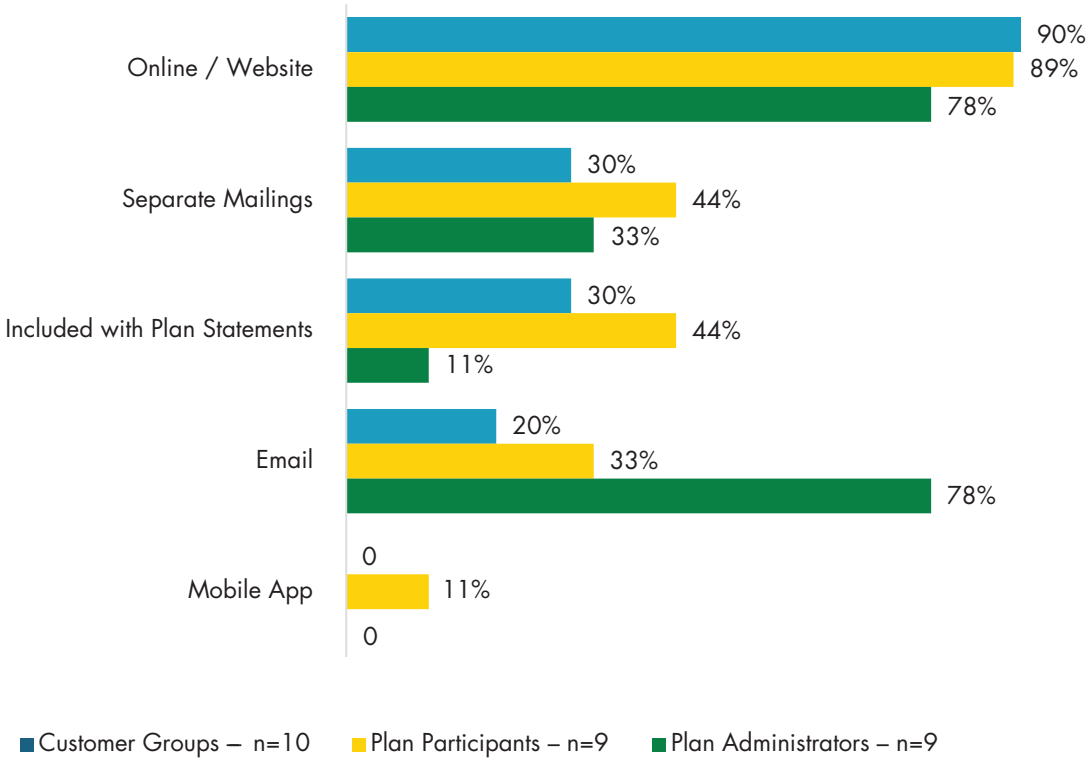
A significant portion of companies (73 percent) do not regularly offer financial-crimes and fraud awareness training or educational materials to their customer groups. Less than 20 percent of companies extend fraud _training or educational resources to policy or contract owners (17 percent), plan administrators and sponsors (15 percent), or plan participants. This limited outreach suggests that many organizations may be missing an important opportunity to strengthen fraud prevention beyond internal controls. Since customers are often the first point of contact for fraud attempts, expanding awareness efforts could help reduce vulnerability to social engineering schemes, account takeover attempts, and identity based fraud — ultimately improving protection for both customers and the companies that serve them (see Figure 22).

Figure 22 — Training or Education for Customer Groups



Companies use a mix of channels to communicate with customer groups, plan participants, and plan administrators, with online/website delivery being the most widely used across all three groups. Online/website channels reach 90 percent of customer groups, 89 percent of plan participants, and 78 percent of plan administrators. Email is also common for plan administrators (78 percent) but is used less frequently for customer groups (20 percent) and plan participants (33 percent). Separate mailings and inclusion with plan statements vary by audience depending on the group. Mobile app delivery remains limited, appearing only for 11 percent of plan participants and not used at all for customer groups or plan administrators See Figure 23).

Figure 23 — Delivery of Training or Educational Materials



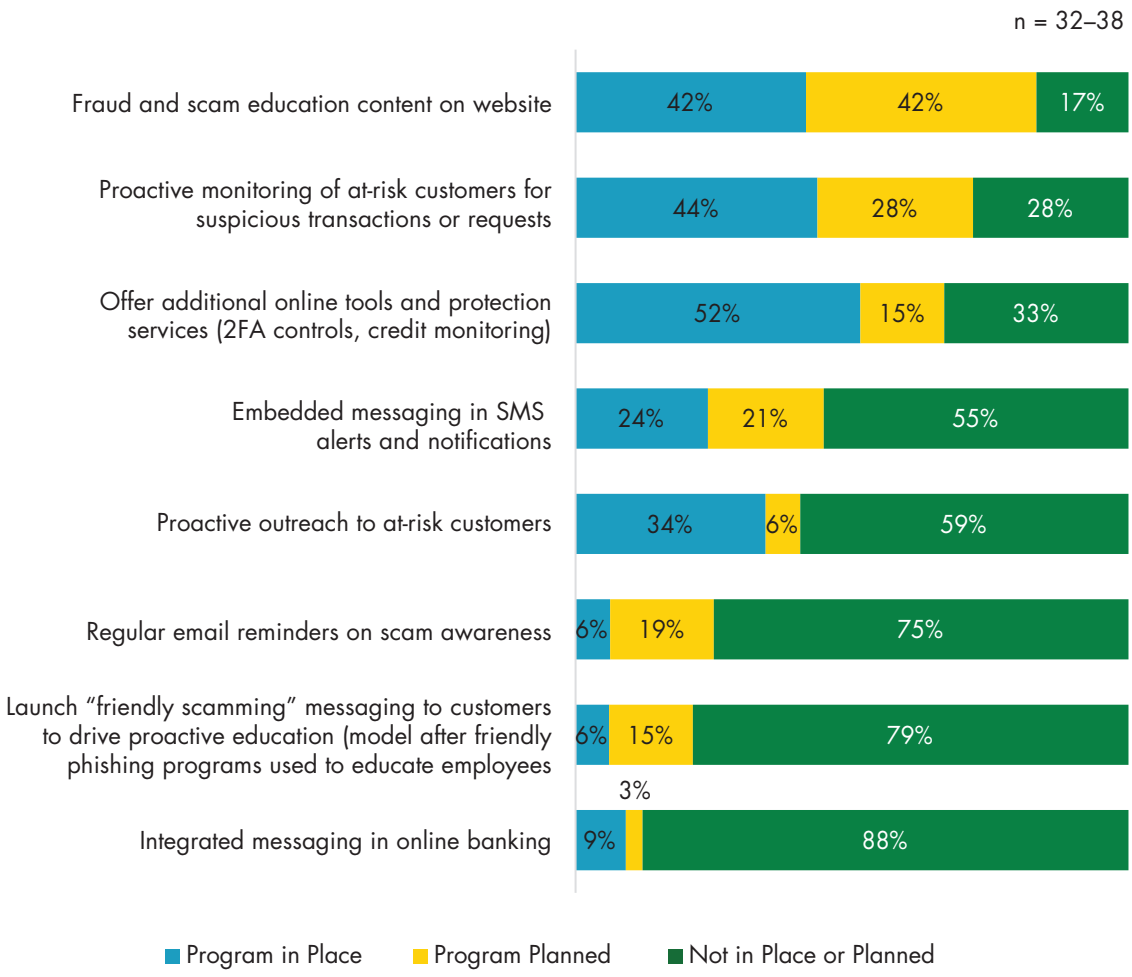
Confidence Scams

To address the growing concern of confidence scams, companies are beginning to focus more on education and protection programs. However, only 25 percent currently have such programs in place, while 41 percent plan to offer them in the future. More than a third (34 percent) neither offer these programs nor plan to, revealing a substantial gap in customer facing fraud prevention efforts. This limited adoption suggests that many organizations may be underestimating the value of proactive customer education — especially as confidence scams continue to rise and often target individuals who are least equipped to identify manipulation. Scalable "always on" tactics remain underutilized — integrated in site/app messaging, regular email reminders, and simulated "friendly scamming" education each show very low current adoption — leaving quick win opportunities on the table.

Among companies that do invest in these initiatives, the most common approach is providing additional online tools and protection services, such as two factor authentication and credit monitoring, with 52 percent offering these capabilities. Another 44 percent engage in proactive monitoring of at risk customers for suspicious transactions or requests. Additionally, 42 percent plan to add fraud and scam education content to their websites (see Figure 24). These initiatives reflect a growing recognition that fraud mitigation must extend beyond internal controls to include active customer support and awareness — especially for those who may be more vulnerable.

Despite this progress, a significant portion of companies still do not prioritize these types of programs, which highlights an area where further investment could greatly enhance customer protection. Encouragingly, 95 percent of companies believe the industry should take a more proactive approach in educating and protecting vulnerable customers from confidence scams. This near unanimous viewpoint signals a strong industry mandate to elevate customer facing fraud prevention strategies and build more comprehensive protection frameworks that extend beyond internal operations.

Figure 24 — Confidence Scam Education and Protection Programs



Challenges and Focus

Insurance company fraud units are operating amid converging pressures, with organizations identifying the need to balance a seamless customer experience with appropriate vigilance (51 percent) and strengthening authentication and identity security (47 percent) as their most pressing challenges, followed closely by the growing impact of AI on fraud prevention and risk management (44 percent). Additional difficulties include technology limitations, emerging fraud schemes, and ongoing resource optimization needs. In response to this landscape, companies are increasingly prioritizing initiatives that modernize fraud prevention while reinforcing organizational resilience, signaling a broader shift toward digitally enabled, risk based operating models.

To address these challenges, insurers are accelerating investments in technology and vendor solutions and placing strong emphasis on workforce enablement, supported by enhanced governance, controls, and identity security frameworks. Fraud units are expanding the use of advanced data analytics and AI driven tools to improve detection, risk scoring, and investigative efficiency, while implementing multifactor authentication, biometrics, improved know-your-customer (KYC) processes, and zero trust security models to reduce identity related risk. These efforts are reinforced by formal governance structures such as AI oversight committees, fraud roadmaps, and ongoing risk assessments to ensure responsible adoption. At the same time, organizations are strengthening employee training, awareness programs, and specialized staffing, and increasing collaboration with industry peers and third parties. Collectively, these actions reflect a strategic focus on strengthening digital defenses, improving execution capabilities, and maintaining a customer centric experience in an increasingly complex fraud environment (see Table 5).

Table 5 — Current Top Challenges and Top Initiatives in 2026

Top Challenges	n = 59	Initiatives	n = 44
Increasing and/or evolving fraud schemes and fraudster capabilities	51%	Technology and Vendor Implementations	61%
Resources (dollars and people)	47%	Workforce Enablement	43%
Internal: challenges, engagement, and prioritization	44%	Governance, Controls and Risk Management	36%
Technology capabilities and adoption	41%	Identity, Security and Authentication	36%
Emerging fraud schemes and threats	32%	AI Solutions and Innovation	34%
Resource allocation and optimization	31%	Organizational and Operating Model Changes	20%
Employee awareness and vigilance	17%	Data, Analytics and Intelligence	18%
Data quality and reliability	15%	External Engagement	16%
Advanced data analytics and insights	12%	Customer Engagement and Awareness	7%
Internal challenges and strategic alignment	8%		
Other	2%		

Outlook

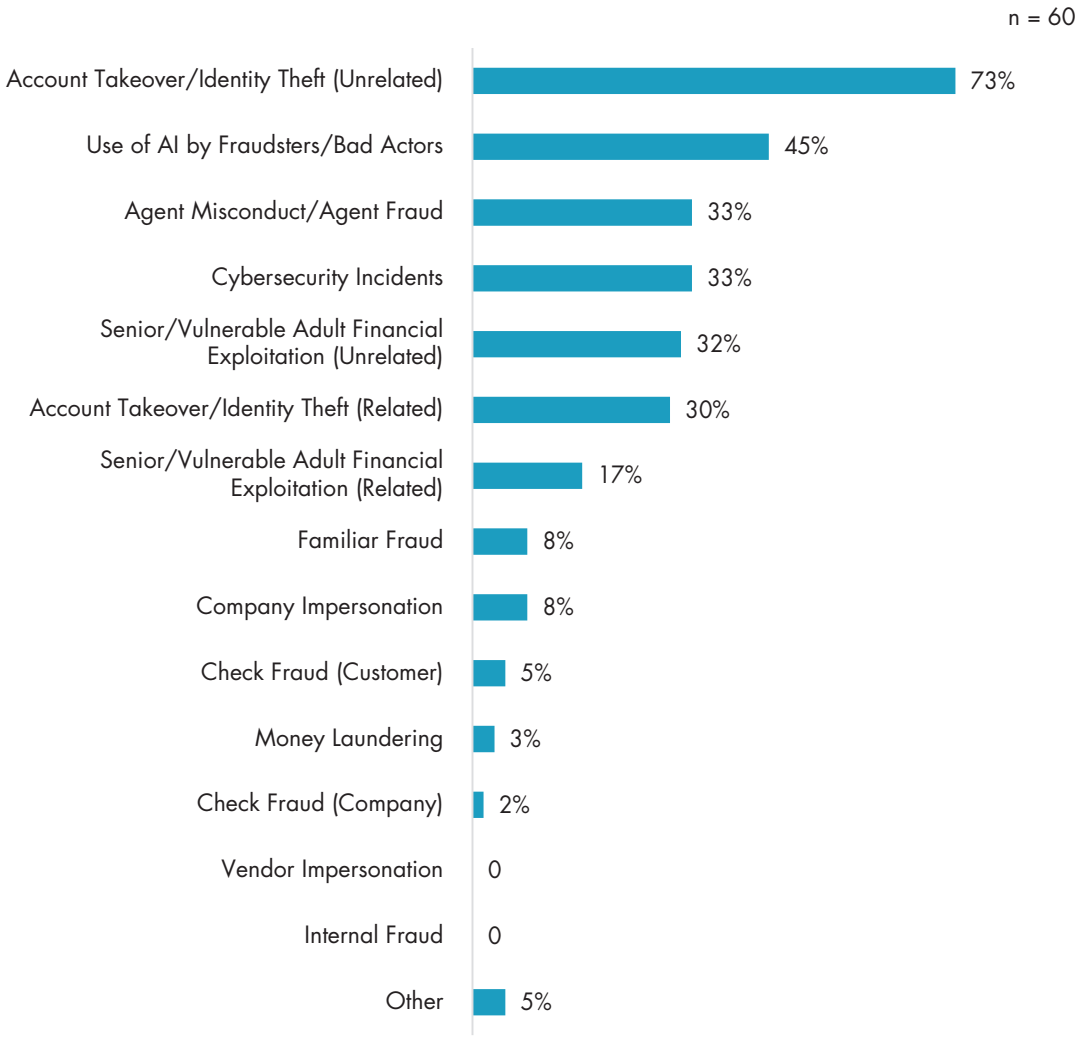
When companies were asked to identify their top three anticipated fraud related challenges for 2026, account takeover/ identity theft (unrelated) incidents emerged as the most pressing concern, cited by 73 percent of respondents. This strong expectation reflects the ongoing escalation of identity based attacks and highlights how increasingly sophisticated impersonation techniques are outpacing traditional verification controls. The prominence of account takeover as a predicted challenge suggests that companies will need to continue strengthening authentication, customer verification processes, and monitoring capabilities to stay ahead of evolving threat patterns.

The expected use of AI by fraudsters also rose sharply. It increased from 28 percent in the 2004 report (projecting to 2025) to 45 percent in the 2025 report projecting to 2026. This rapid jump reflects the industry-wide recognition that generative AI, deepfakes, voice cloning, and automated social engineering tools are making fraud attempts more convincing, scalable, and difficult to detect. The trend underscores that adversaries are adopting advanced technologies faster than many organizations can deploy defensive tools, creating urgency for companies to modernize analytics, adopt AI-enabled detection, and reinforce governance frameworks around emerging threats.

Agent misconduct/ agent fraud (33 percent), along with cybersecurity incidents (33 percent), remain significant concerns and closely mirror results from the 2024 report. Their persistence illustrates the dual nature of fraud risk: Both internal vulnerabilities and external digital threats continue to evolve in parallel. Companies may need to deepen their focus on internal controls, strengthen agent oversight, enhance cybersecurity resilience, and ensure coordinated fraud and cyber response strategies to manage these interconnected risks effectively (see Figure 25).

Although check fraud incidents (customer and company) were higher in the 2024 report than in the 2023 report, they are not expected to be major issues in 2026 based on this year's responses. This shift suggests that investments in check fraud controls — and the ongoing decline in check usage — are reducing exposure. However, the deprioritization of check fraud also implies that fraudsters may be moving toward faster and more digitally oriented channels, placing greater pressure on companies to shore up controls in areas where exploitation is easier and detection is more challenging.

Figure 25 — Top Three Most Challenging Financial Fraud Exposures Anticipated in 2026



In 2026, companies expect to place continued emphasis on strengthening authentication processes and control enhancements, with 54 percent ranking this focus among their top three priorities and 20 percent identifying it as their single highest priority. This sustained attention reflects the industry's recognition that authentication remains one of the most effective defenses against identity based fraud, account takeover, and increasingly sophisticated impersonation schemes.

At the same time, companies are accelerating their interest in AI-enabled solutions. Using AI to enhance fraud prevention or authentication capabilities is the top priority for 25 percent of organizations and appears in the top three priorities for 48 percent. Among larger companies, this trend is even more pronounced: 41 percent list AI-driven fraud and authentication enhancements as their highest priority, and another 29 percent place authentication process improvements at the top. These patterns suggest that larger organizations — with greater resources and broader digital footprints — are moving more aggressively toward advanced, scalable technologies capable of analyzing complex behaviors and detecting fraud patterns that traditional controls may miss.

Training and education for employees also remain key areas of focus, with 67 percent of companies identifying these efforts as important. However, only 7 percent rank training as their top priority, and just 34 percent include it in their top three. This gap indicates that while organizations recognize the value of employee awareness, they may be prioritizing technology driven capabilities over human centric defenses. As fraud schemes become more sophisticated — and often rely on social engineering — this lower prioritization could create vulnerabilities if training programs do not evolve in tandem with technological investments (see Figure 25).

Together, these priorities reveal a strategic industry shift: companies are increasingly relying on technology, particularly AI and enhanced authentication controls, to stay ahead of fraud. However, the comparatively lower prioritization of employee training suggests that some organizations may be underestimating the role of human behavior in both creating and preventing fraud risk. Balancing cutting edge tools with strong, ongoing education will be essential to building comprehensive, resilient fraud prevention programs in the years ahead (see Table 6).

Table 6 — Areas of Focus for 2026

	Areas of Focus for 2026			
	Top Priority	2nd Priority	3rd Priority	A Focus
Using AI to enhance fraud prevention or authentication capabilities	25%	5%	18%	62%
Authentication Process and Control Enhancements	20%	19%	14%	65%
Digital (e.g., online, and mobile) Fraud Process and Control Enhancements	7%	25%	12%	50%
Training and Education for employees	7%	11%	16%	67%
Technology — Internal Solutions	7%	9%	5%	45%
Initiate a Fraud Risk Assessment	7%	0	4%	18%
Technology — External Solutions	5%	9%	4%	32%
Disbursement Process and Control Enhancements	5%	5%	7%	30%
Orchestration Layer/Integration Hub	5%	2%	2%	17%
Enhancing Management Reporting	3%	4%	14%	40%
Update Your Current Fraud Risk Assessment	3%	2%	2%	27%
Governance Model	2%	2%	2%	17%
Centralizing the Organizational Structure	2%	2%	0	8%
Training and Education for agents/field representatives	0	7%	2%	22%
Training and Education for consumers	0	0	0	20%
Other (please specify):	2%	0	0	3%

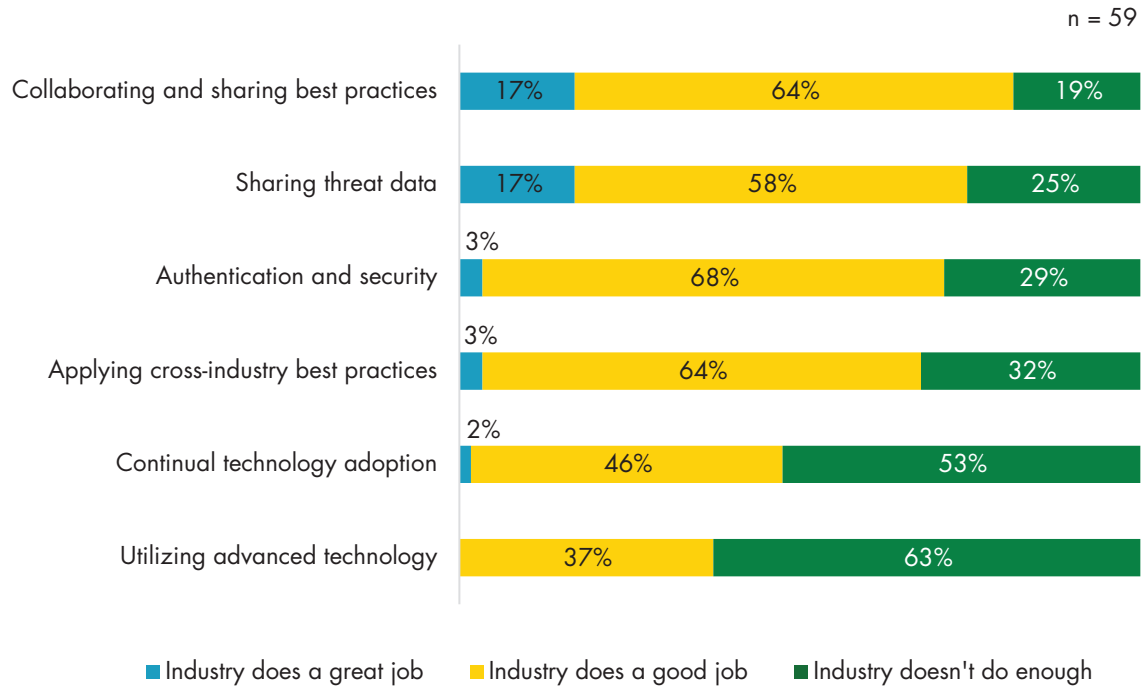
The Industry

In 2025, opinions are divided on whether the Insurance and Retirement Services industry is keeping pace with other sectors in adopting tools and technologies to combat fraud. Fifty five percent of respondents believe the industry is keeping up, while 45 percent feel it is falling behind — and this concern is more pronounced among larger companies, where 59 percent say the industry is not keeping pace. This split perspective suggests growing pressure on organizations to modernize, particularly as larger carriers — with more complex operations and greater exposure — may better recognize the accelerating technological advancements seen in other industries.

Despite this divide, most companies believe the industry performs well in key collaborative areas. Eighty-one percent say the industry does a great or good job combating fraud through collaboration, and 75 percent cite strong performance in sharing best practices and threat data. This confidence reflects the industry's long standing reliance on collective intelligence and cooperative initiatives as foundational elements of fraud prevention (see Figure 26).

At the same time, respondents believe the industry has room for improvement — particularly in how it adopts and applies technology. Fifty-three percent say the industry needs to improve in continuous technology adoption, and 63 percent believe it could better leverage advanced technologies. These sentiments highlight a critical implication: while collaborative practices remain strong, companies increasingly recognize that collaboration alone is not enough. Enhanced and sustained investment in modern tools, advanced analytics, and emerging technologies will be essential for the industry to keep pace with rapidly evolving fraud schemes and technology enabled threats.

Figure 26 — Industry Actions Evaluation



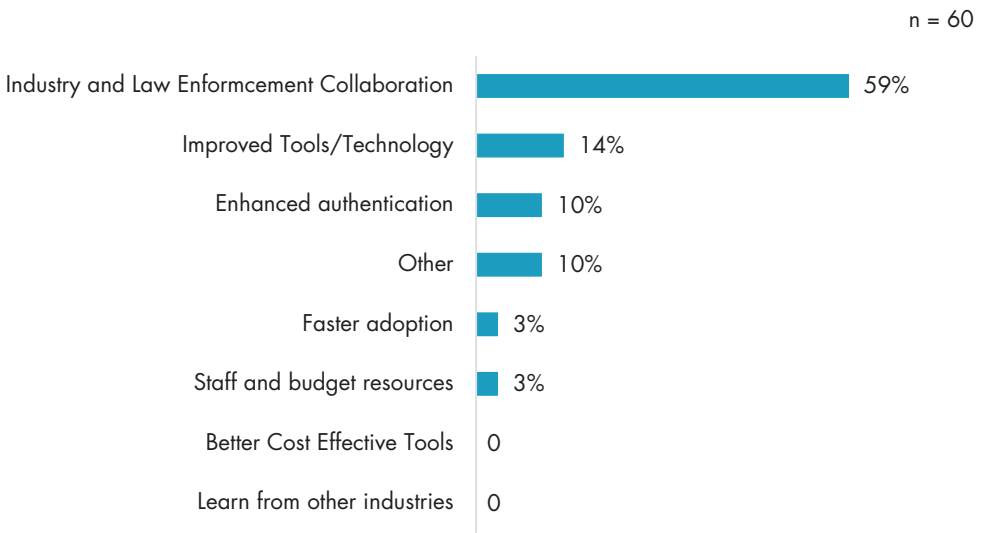
Strategic Insight:

The Insurance and Retirement Services industry remains strong in collaboration and information sharing, but opinions are increasingly divided on whether it is keeping pace with other sectors in adopting advanced fraud-fighting technologies — especially among larger, more complex carriers. While collective efforts with peers and law enforcement are viewed as the most urgent and effective lever for combating fraud, respondents broadly acknowledge that collaboration alone is no longer sufficient.

Sustained investment in modern tools, AI-enabled analytics, and integrated detection capabilities — combined with deeper, standardized data sharing — will be critical to keep pace with rapidly evolving, technology-driven fraud threats.

Collaboration with law enforcement and across the industry is identified as the most urgent action needed to better combat fraud, representing the clear top priority. There is strong emphasis on deeper information sharing, including expanding cross carrier groups such as LIMRA and LOMA Financial Crimes Services, strengthening collaboration tools like FraudShare, and sharing non customer specific fraud data, loss data, and emerging threat trends to create greater collective impact. Improved alignment with law enforcement resources, as well as cooperation with banks and other financial institutions, is also viewed as critical, reflecting the reality that fraud frequently spans multiple sectors. Beyond collaboration, improved tools and technology (14 percent) are highlighted through the need for greater use of AI, more integrated fraud detection solutions, and enhancements to bank verification and automated clearinghouse (ACH) processes to keep pace with rapidly evolving fraud schemes. Overall, while technology and controls remain important, the industry places greatest value on stronger, more coordinated collaboration supported by effective data sharing, regulatory alignment, and collective tools to strengthen fraud and financial crime protection.

Figure 27 — Industry Actions Needed



Conclusion

The 2025 Financial Crimes and Fraud Prevention Benchmarking Survey reveals an industry confronting increasingly sophisticated threats with a heightened sense of urgency and commitment. Fraud incidents continue to rise across nearly all categories, fueled in part by rapid advancements in AI that are enabling more convincing impersonation, manipulation, and social engineering attacks. While organizations have made meaningful progress in maturing their programs — particularly in governance, reporting, and the use of data for monitoring — many still face foundational challenges, including fragmented structures, resource constraints, inconsistent risk management practices, and uneven adoption of advanced technologies. The growing exposure of seniors and vulnerable adults, the acceleration of identity based attacks, and the widening gap between large and small companies further underscore the need for continued investment and modernization.

Despite these challenges, the industry demonstrates strong alignment on several priorities. Companies are increasingly focused on strengthening authentication controls, enhancing digital and mobile defenses, and exploring AI enabled fraud prevention capabilities. Collaboration also remains a defining strength: carriers continue to value shared intelligence, collective defense, and cross industry cooperation as essential components of an effective fraud prevention strategy. However, the survey also highlights that collaboration alone is not enough — modern analytics, unified data environments, and scalable technologies must accompany these efforts to keep pace with rapidly evolving threats.

Looking ahead, the industry must balance advanced technological investment with human centered defenses. Employee vigilance, customer education, and targeted awareness programs remain critical but underutilized components of a comprehensive strategy. As fraudsters continue to innovate, organizations that fail to evolve both technologically and operationally risk falling behind. The path forward requires not only stronger controls and smarter tools but also clearer governance, more consistent risk assessment, and a sustained commitment to enterprise wide fraud resilience.

Ultimately, the findings of this report reinforce a central message: **Fraud prevention is no longer a static function but a continuously advancing discipline**. Companies that prioritize adaptability, collaboration, and innovation will be best positioned to protect their customers, their reputations, and the broader financial ecosystem in the years ahead.

Appendix A — Participating Companies

The following is a list of the 60 companies that participated in this year's survey, along with their years of participation. The 22 highlighted companies have participated in all six years of the survey.

AAA Life Insurance Company (2024-2025)

Aflac (2022 – 2025)

Allianz Life Insurance North America (2020 – 2025)

American Equity (2025)

American Family Life Insurance Company (2020 – 2025)

American National Insurance Company (2022, 2025)

Americo Life (2022 – 2025)

Ameritas (2020, 2022 – 2023, 2025)

Athene USA (2020 – 2025)

Banner Life Insurance Company/Legal and General America (2022 – 2025)

Brighthouse Financial (2020 – 2025)

Cincinnati Life (2020, 2025)

CNO Financial Group (2021 – 2023, 2025)

Empower (2022 – 2023, 2025)

Equitable (2021 – 2025)

Everlake Life Insurance Company (2021 – 2025)

F&G Annuities & Life, Inc. (2022 – 2025)

Foresters Financial (2020 – 2021, 2023 – 2025)

Group 1001 (2020 – 2022, 2024 – 2025)

Guardian Life Insurance Company of America (2021 – 2025)

John Hancock Life Insurance Company (2020 – 2021, 2024 – 2025)

KKR/Global Atlantic (2021, 2023, 2025)

Kuvare (2023 – 2025)

Lincoln Financial Group (2020 – 2025)

MassMutual (2020 – 2025)

MissionSquare Retirement (2023 – 2025)

Modern Woodmen of America (2020, 2023 – 2025)

Nassau Financial Group (2024 – 2025)

National Life Group (2020 – 2025)

Nationwide Insurance (2020 – 2025)

New York Life Insurance Company (2020 – 2021, 2023 – 2025)

Northwestern Mutual Life Insurance Company (2020 – 2025)

NSS Life (2022, 2025)

OneAmerica Financial (2020 – 2025)

Pacific Life Insurance Company (2020 – 2025)

Physicians Mutual Life (2025)

Principal Financial Group (2024 – 2025)

Protective Life Insurance Company (2020 – 2021, 2023 – 2025)

Prudential Insurance Company of America (2020 – 2025)

Reliance Standard Life Insurance, USA (2025)

Sagicor Life Insurance Company (2020, 2024 – 2025)

Sammons Financial Group (2020 – 2025)

Securian Financial Group (2020 – 2022, 2024 – 2025)

Security Benefit Life Insurance Company (2023 – 2025)

Security Mutual Life of New York (2025)

Southern Farm Bureau Life Insurance Company (2020 – 2025)

Standard Insurance Company (2020 – 2025)

State Farm Life Insurance Company (2022 – 2025)

Sun Life Assurance Company of Canada (US) (2020 – 2025)

Symetra Life Insurance Company (2020 – 2025)

T. Rowe Price Associates (2020 – 2025)

Talcott Financial Group (2020 – 2025)

The Canada Life Assurance Company (2021 – 2025)

The Savings Bank Mutual Life Insurance Co of MA (2020, 2022 – 2025)

Thrivent Financial for Lutherans (2020 – 2025)

Transamerica Life Insurance Company (2021 – 2025)

TruStage (2020 – 2025)

Venerable Insurance and Annuity Company (2020 – 2025)

Voya Financial, Inc. (2021 – 2025)

Western & Southern Financial Group (2021, 2024 – 2025)

Appendix B — Definitions

Fraud Types

Account Takeover (Related) — Unauthorized attempt to access a customer account by a related party (e.g., family member, friend, caregiver etc.) impersonating the customer to fraudulently obtain data or funds.

Account Takeover (Related) — Unauthorized attempt to access a customer account by a related party (e.g., family member, friend, caregiver etc.) impersonating the customer to fraudulently obtain data or funds.

Account Takeover (Unrelated) — Unauthorized attempt to access a customer account by an unknown and unrelated third-party imposter to fraudulently obtain data or funds.

Agent Fraud — Any fraudulent activity undertaken by the agent to increase their compensation or receive funds and\or misrepresent product or service terms or conditions for personal gain.

Check Fraud (Company) — Intentionally forging check signatures or endorsements, altering check payees, or creating unauthorized checks for the purpose of fraudulently obtaining Company funds. Example: A fraudster creates counterfeit checks using your company's name and banking information and uses them to purchase goods from someone they met on social media.

Check Fraud (Customer) — Forging check signatures or endorsements, altering check payees, for the purpose of fraudulently obtaining customer funds. Example: A fraudster obtains a legitimately issued check payable to a customer and alters the payee's name in order to cash it.

Claims Fraud — Intentionally submitting false or misrepresented information to generate or support a claim (all life, health, disability, annuity, and retirement services products).

Company Impersonation — Impersonations of company or associated party (employee, agent, vendor) to obtain information or funds from an individual or company that may or may not be a customer or employee of the company. Example: A fraudster calling random people impersonating your company to obtain their personal data and\or account information.

Confidence Schemes — Situations in which a fraudster obtains a customer's trust through deception to persuade them into giving them information or money (e.g., Romance, IRS, help desk, or lottery scams).

Employee Impersonation — Impersonation of an employee to obtain the employee's data or to redirect payroll or expense reimbursements. Example: A fraudster impersonates an employee and contacts the HR department to update the employee's banking information to an account they control.

Internal Fraud — Fraudulent acts perpetrated by employees or contractors to obtain company or customer data and/or funds.

Money Laundering — Engaging in acts designed to conceal or disguise the true origins of derived proceeds so that the unlawful proceeds appear to have been derived from legitimate origins and constitute legitimate assets (Only Confirmed).

New Business/Application Fraud — Agent or customer intentionally providing false information, omitting, or understating material information to obtain an insurance policy or securities account that would not have been approved during the policy underwriting or account application processes if accurate and/or complete information had been provided.

Senior and Vulnerable Adults (Related) — A person with functional, physical, or mental inability to care for self or someone who is unable to protect themselves against harm or financial exploitation perpetrated by a known or related party (e.g., family member, friend, or caregiver).

Senior and Vulnerable Adults (Unrelated) — A person with functional, physical, or mental inability to care for self or someone who is unable to protect themselves against harm or financial exploitation perpetrated by an unknown or unrelated party. Example: A fraudster contacts or befriends the victim and executes a confidence scam (e.g., romance, IRS, help desk or lottery).

Vendor Impersonation — Impersonations of a company vendor or supplier to obtain company funds or data. Example: A fraudster submits bogus invoices or updates legitimate invoices with their bank information to redirect payments to an account they control.

Organizational Structures

Centralized — A single department or function handles all financial crimes services or fraud-prevention functions for all business lines.

Partially Centralized — A single department or function has oversight and governance over other departments or functions with financial crimes services or fraud-prevention responsibilities that report into other departments or product lines.

Decentralized — Multiple departments or functions handle financial crimes services or fraud-prevention functions and report into different departments or product lines with no centralized governance or oversight.

Program Maturity

Ad-Hoc — Fraud events are handled in a reactive and ad-hoc manner at the local level with minimal documented policies or procedures.

Initial — Fraud events are handled in a reactive manner at the local level with some enterprisewide coordination, policies, and procedures are documented. Fraud controls are mainly detective and risk assessment process is ad-hoc (if existent).

Operational — Fraud events are handled in a coordinated manner with documented policies and procedures. Fraud controls are documented and consist of both detective and preventative. There is an enterprise perspective with at least some governance and risk assessment practices driving the program.

Optimal — A defined governance and risk assessment process drives the financial crimes and fraud prevention program with an enterprise perspective. Procedures, policies, and controls are well documented with a focus on prevention and continual improvement.

Data Maturity

Ad hoc — Basic reporting provides raw data for human analysis.

Exception — Alerts generated based on known exceptions or threat indicators.

Monitoring — Alerts generated based on trend and pattern analysis that detect unusual interactions and\or transactions.

Optimal — Program utilizes advanced analytics to identify or predict fraudulent activity in near real time.

AI Maturity

Awareness — Aware of AI capabilities though have yet to begin evaluating, experimenting, or implementing any AI capabilities.

Evaluation — Evaluating AI tools and capabilities to determine how they could be used to enhance our fraud prevention program.

Experimenting — Testing AI capabilities though none have been implemented in production.

Initial — Implemented some AI use cases with results still being evaluated.

Operational — Implemented some AI use cases in production with positive results.

Transformative — Implemented multiple AI use cases with consequential and positive results.

Advancing the financial services industry by empowering our members with

LIMRA LOMA
Navigate With Confidence

0433-2026