Financial Crimes Services and Fraud Prevention

Benchmarking Study

Executive Summary

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.

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

LIMRA
Navigate With Confidence

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' abilities 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 who 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 IVRs 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 underinvest 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.