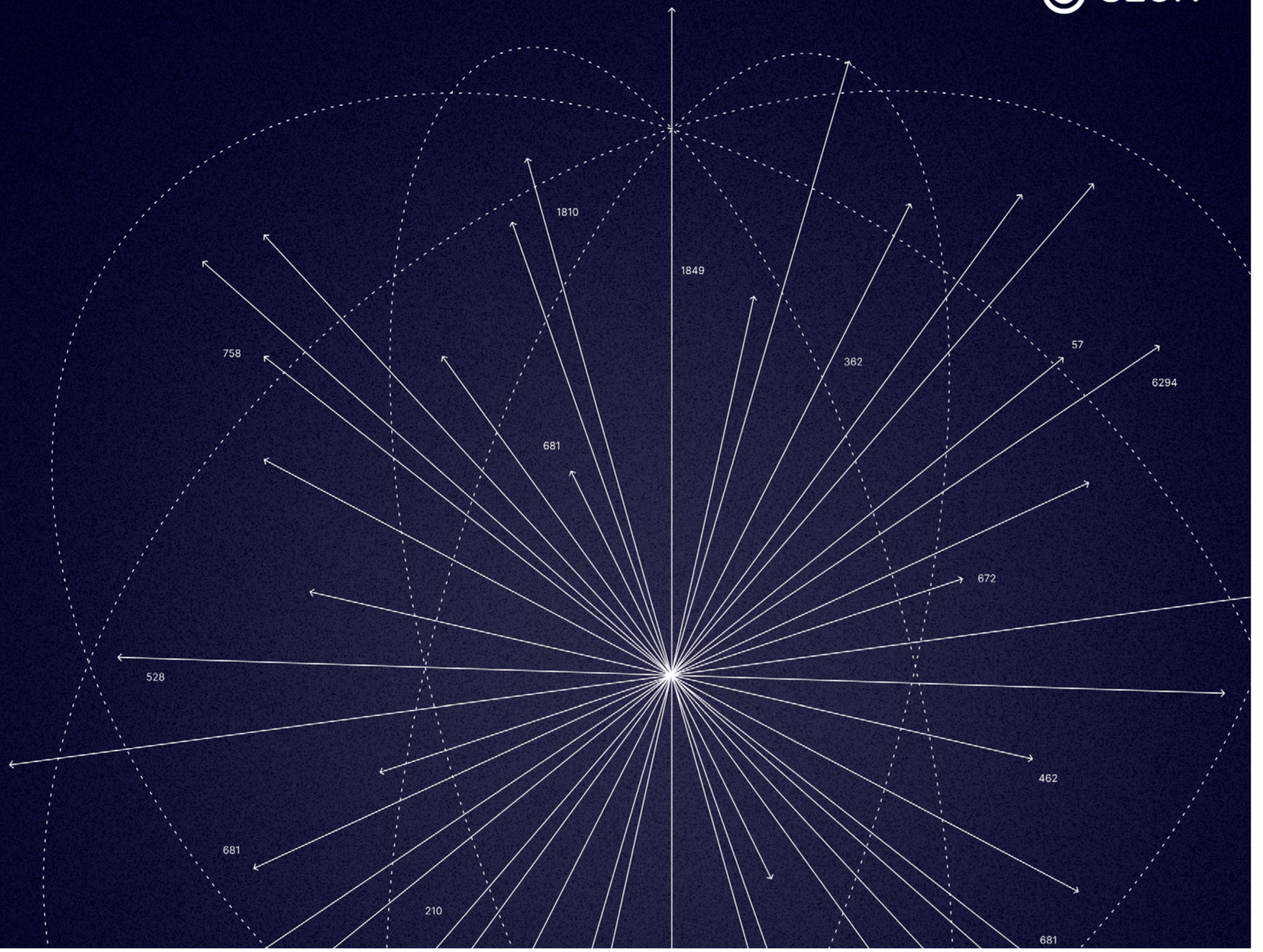
2025 Digital Fraud Outlook



A Global Fraud, Risk & Compliance Trend Report

Table of Contents

A Note From Our CEO

As we progress through 2025, the digital economy will continue to bring extraordinary opportunities and complex challenges in fraud prevention. We are witnessing the landscape of fraud and financial crime evolving at speed, requiring increasingly sophisticated solutions.

This year's **Global Digital Fraud Outlook** report comes at a crucial moment. Our extensive research across payments, financial services, fintech, iGaming and eCommerce sectors reveals a clear message: solutions that rely on detection alone are no longer sufficient in today's real-time economy.

What's notably different this year isn't just the accelerated pace of fraud but also how significantly businesses have had to pivot to AI-driven solutions and automated processes to stay ahead. Yet, it's apparent that technology isn't enough — our findings emphasize that the thoughtful integration of advanced technology with human expertise is truly what moves the fraud prevention needle.

The report's insights go beyond mere data points to include actionable information designed to bolster anti-fraud strategies and investment decisions in technology and personnel, sustain operational agility and move fraud and risk teams closer to more autonomous fraud prevention.

2025 is the year of adaptive fraud prevention — focusing on intelligent, real-time decision-making that balances security, agility and user experience.

Fraud teams must move beyond static defenses to dynamic, context-aware models that continuously adapt in real time. This shift will enable organizations to anticipate threats, respond instantly and refine fraud strategies as risks evolve. We trust these perspectives will prove helpful in your fraud prevention efforts.

Tamás Kádár
Chief Executive Officer, SEON

01

Executive Summary & Methodology

Executive Summary

This report serves as a strategic roadmap for organizations seeking to strengthen their fraud prevention capabilities while balancing security, operational efficiency and customer experience in today's digital economy.

Organizations are prioritizing investments in real-time monitoring capabilities, automated detection systems and advanced analytics. These investments reflect a broader industry shift toward more sophisticated, technology-driven approaches to fraud prevention while maintaining essential human oversight.

1

Fraud Budgets Are Growing, But Tech Investments Should Be Real-Time, Scalable and Automate Workflows

85% of organizations have increased their fraud prevention budgets, and **88%** are expanding their fraud teams. However, businesses must ensure these investments are directed toward the right tools, technology and automation to maximize ROI.

2

Real-Time Transaction Monitoring is the #1 Investment Priority

62% of organizations are shifting away from batch-based transaction monitoring in favor of real-time fraud detection, enabling them to stop fraud before it impacts revenue.

3

Collaboration & Cross-Team Intelligence is a Competitive Advantage

While **97%** of companies recognize IT & Security departments as critical to fraud prevention efforts, **95%** emphasize cross-departmental collaboration with product, marketing and customer service teams to identify and mitigate threats faster.

4

AI & Data Analytics Are the Most Sought-After Fraud Prevention Skills

As fraud tactics grow more sophisticated, **76%** of organizations are prioritizing AI, machine learning and advanced data analytics to build skillsets that enhance detection accuracy and automate risk decisions.

Methodology

We surveyed **574 fraud, risk and compliance professionals** from organizations of varying sizes and industries to understand fraud prevention strategies, benchmarking efforts and emerging trends shaping 2025.

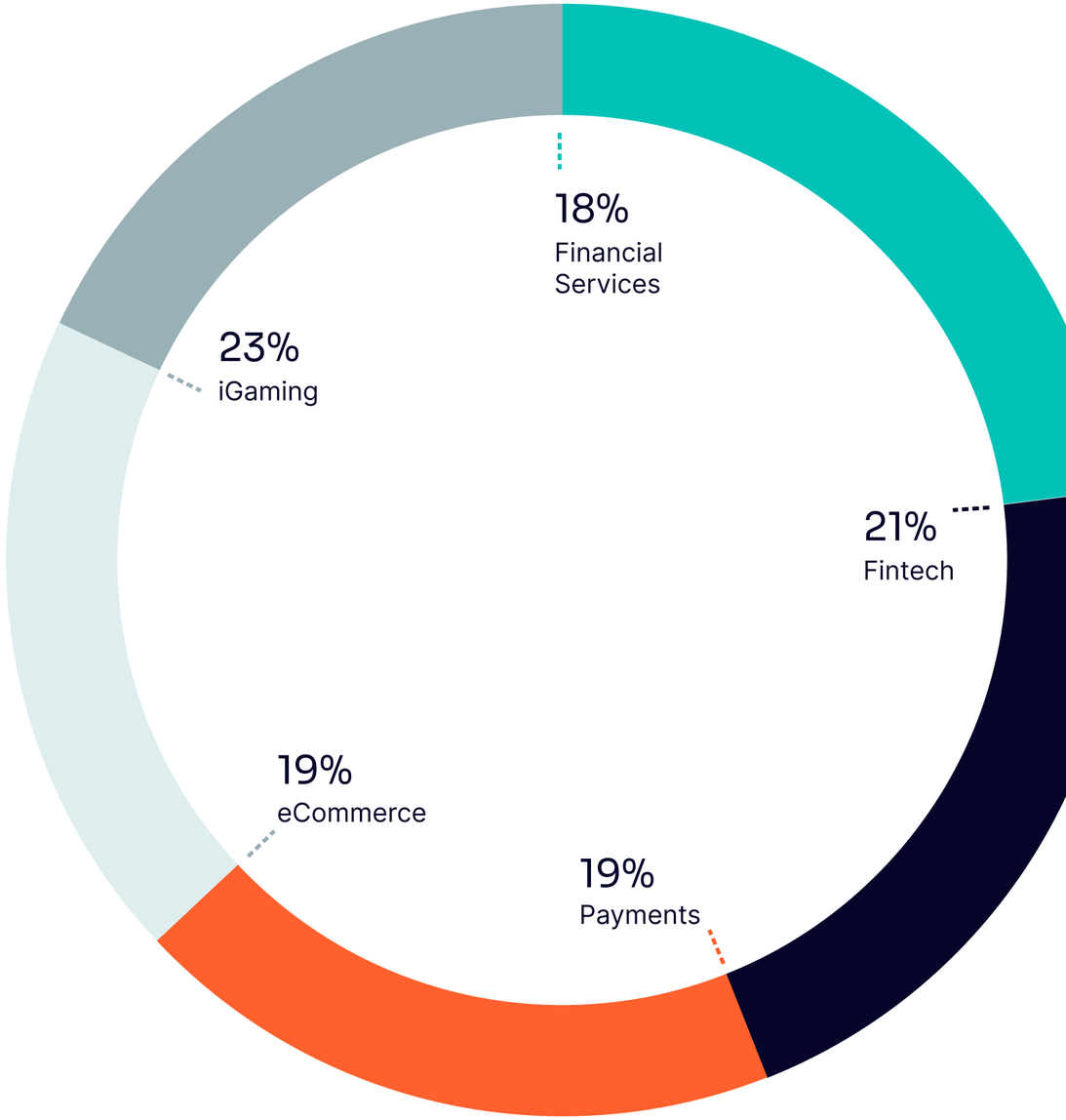
Our respondents represent decision-makers and practitioners from the Financial Services, Fintech and Payments sectors, focusing on consumer-facing digital financial services. Additionally, we surveyed professionals in eCommerce along with perspectives from the iGaming industry, spanning gambling platform providers, operators and social gaming businesses.

We focused on the professionals directly responsible for fraud prevention, risk management, AML compliance and KYC processes within their organizations, ensuring the insights gathered are highly relevant to real-world fraud challenges.

The majority of respondents come from **EMEA (55%)** and **North America (43%)**, with additional insights from **the rest of the world (2%).**

Survey Timeframe: December 2024 - January 2025
Survey Size: 574

Fraud, Risk & Compliance Organization Breakdown



Nearly **50% of respondents hold managerial positions**, with **31% at the director level** and **20% in the C-suite**. This split makes certain that the report reflects perspectives from both strategic decision-makers and those executing fraud prevention initiatives.

⟶ Professional Role Breakdown

Nearly three-quarters of respondents work for companies generating **over $50 million in annual revenue**, making insights relevant to scaling organizations and large enterprises with complex fraud challenges.

⟶ Revenue of Organization

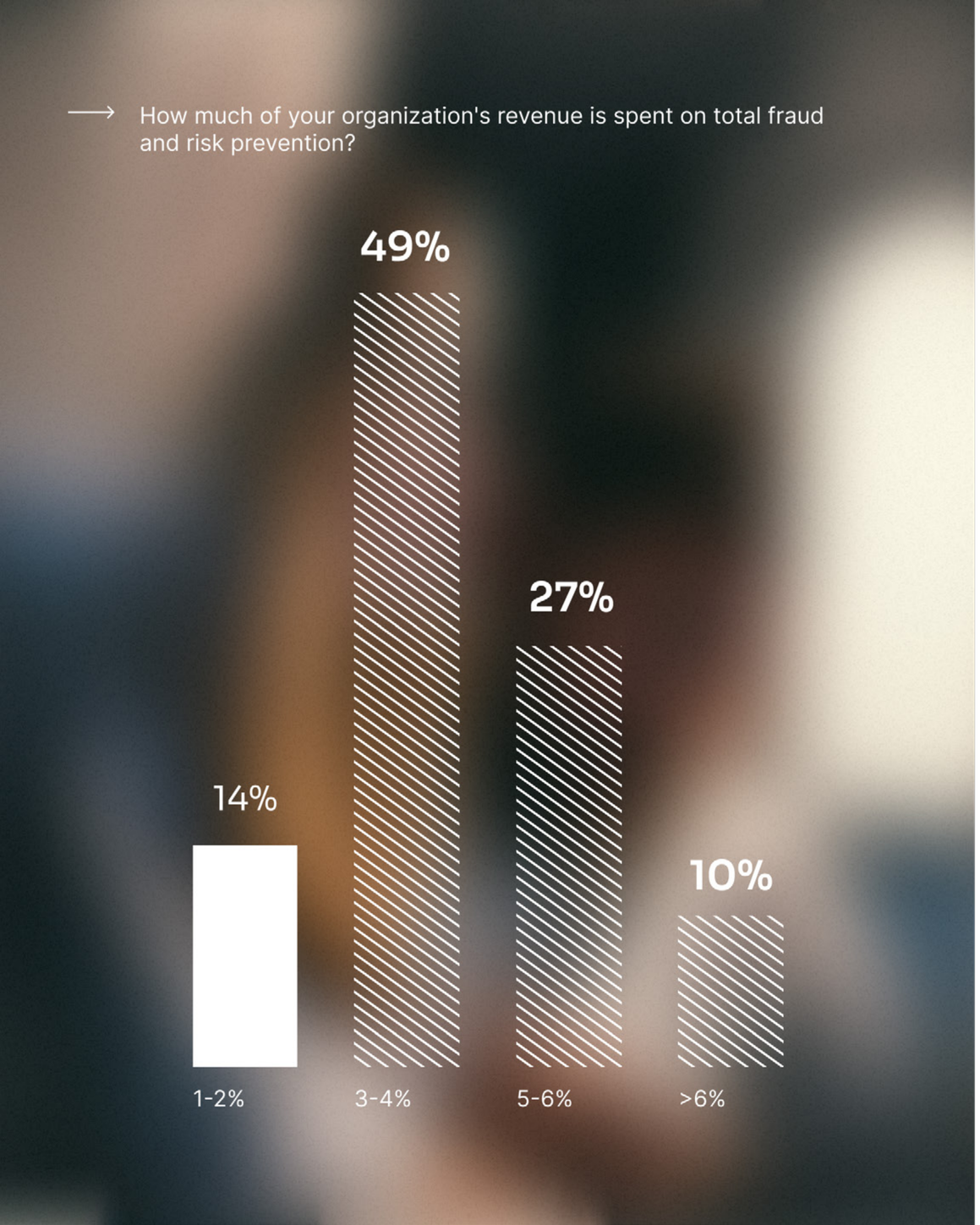
02

Fraud Program Spending is on the Rise

85% of Companies Are Increasing Fraud Budgets

Most organizations measure fraud losses based on direct financial impact — chargebacks, disputes and lost revenue. But fraud's actual opportunity cost extends beyond the obvious. **Businesses may lose up to 5% of their revenue** when factoring in operational inefficiencies, compliance fines and customer churn.

Despite **85% of companies increasing fraud budgets**, many underestimate the long-term financial toll of fraud. In fact, **56% of respondents disagree with the statement that fraud losses are outpacing revenue growth**, suggesting a potential blindspot in how fraud costs are being calculated.



86% of Organizations Spend Over 3% of Revenue on Fraud Prevention

Businesses across verticals are investing heavily in fraud prevention, reflecting fraud attacks' growing complexity and scale.

Even more striking, **86% of respondents report spending over 3% of their revenue** on fraud prevention — but this may not capture the full picture.

With SEON's clients, **we've observed that many organizations define the total cost of fraud differently.** Some only factor in hard costs, such as actual losses and technology, while others include costs that are more difficult to measure, such as reputational damage and negative customer impacts from fraud events.

However, with rising costs, fraud teams must continuously demonstrate ROI by reducing fraud losses, optimizing efficiency and minimizing hidden costs across their organization.

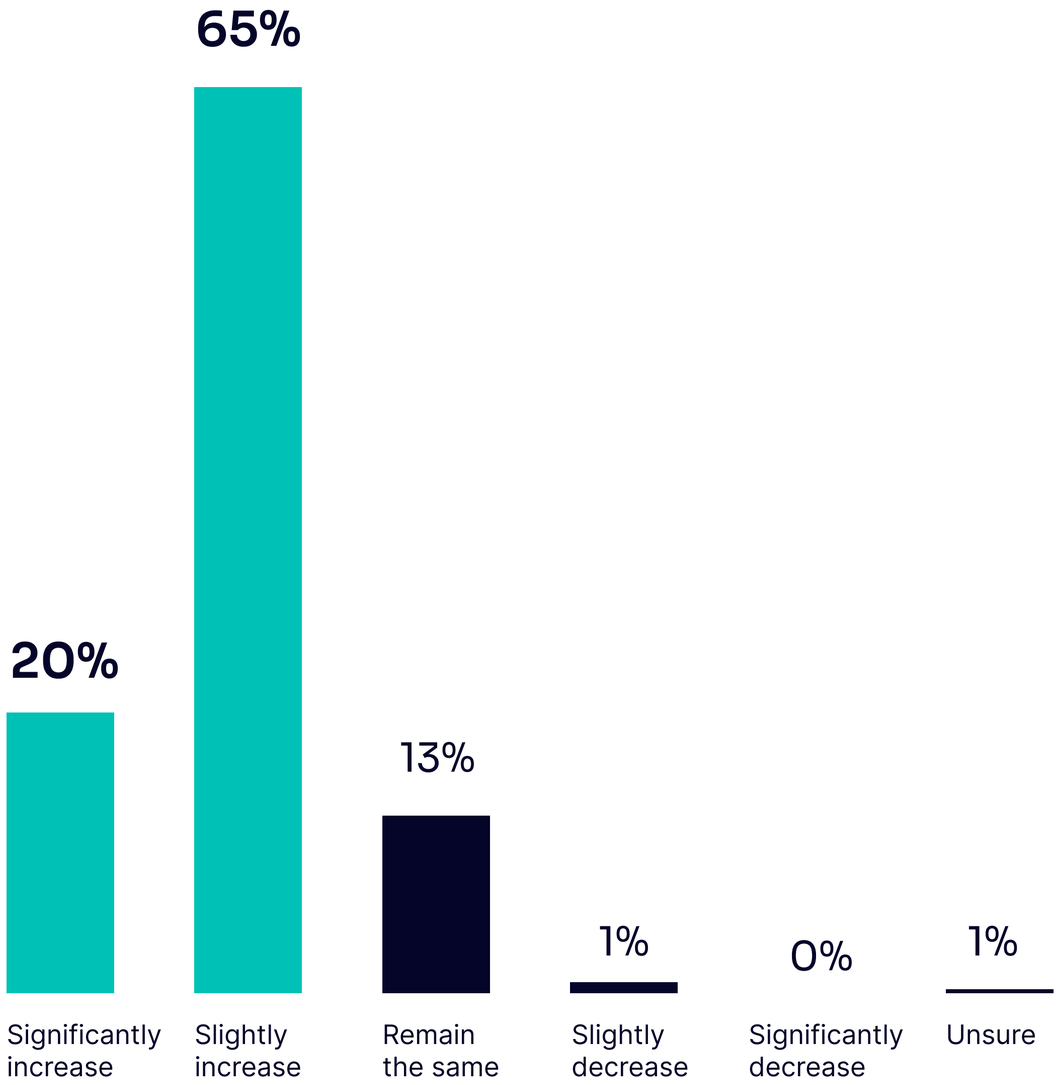
Is Spending More Effective? How Can Companies Ensure Fraud Prevention Budgets Deliver?

Businesses are doubling down on proactive fraud prevention, investing now to avoid higher long-term costs from fraud losses, customer churn and regulatory penalties.

While rising budgets are a sign of commitment, they also highlight the need for efficient resource allocation to ensure investments yield measurable results.

Without a strategic and technology-forward approach, increased budgets won't necessarily lead to more effective fraud prevention — **teams need to focus on real-time detection, automation and transparent AI-driven risk scoring.**

How is your organization's budget for fraud prevention expected to change over the next 12 months?



This trend underscores the growing recognition that fraud prevention requires dedicated resources and expertise.

What This Means:

→ Companies are prioritizing experts as fraud risks escalate

→ Growth varies — some companies are making incremental hires; others have bigger hiring plans

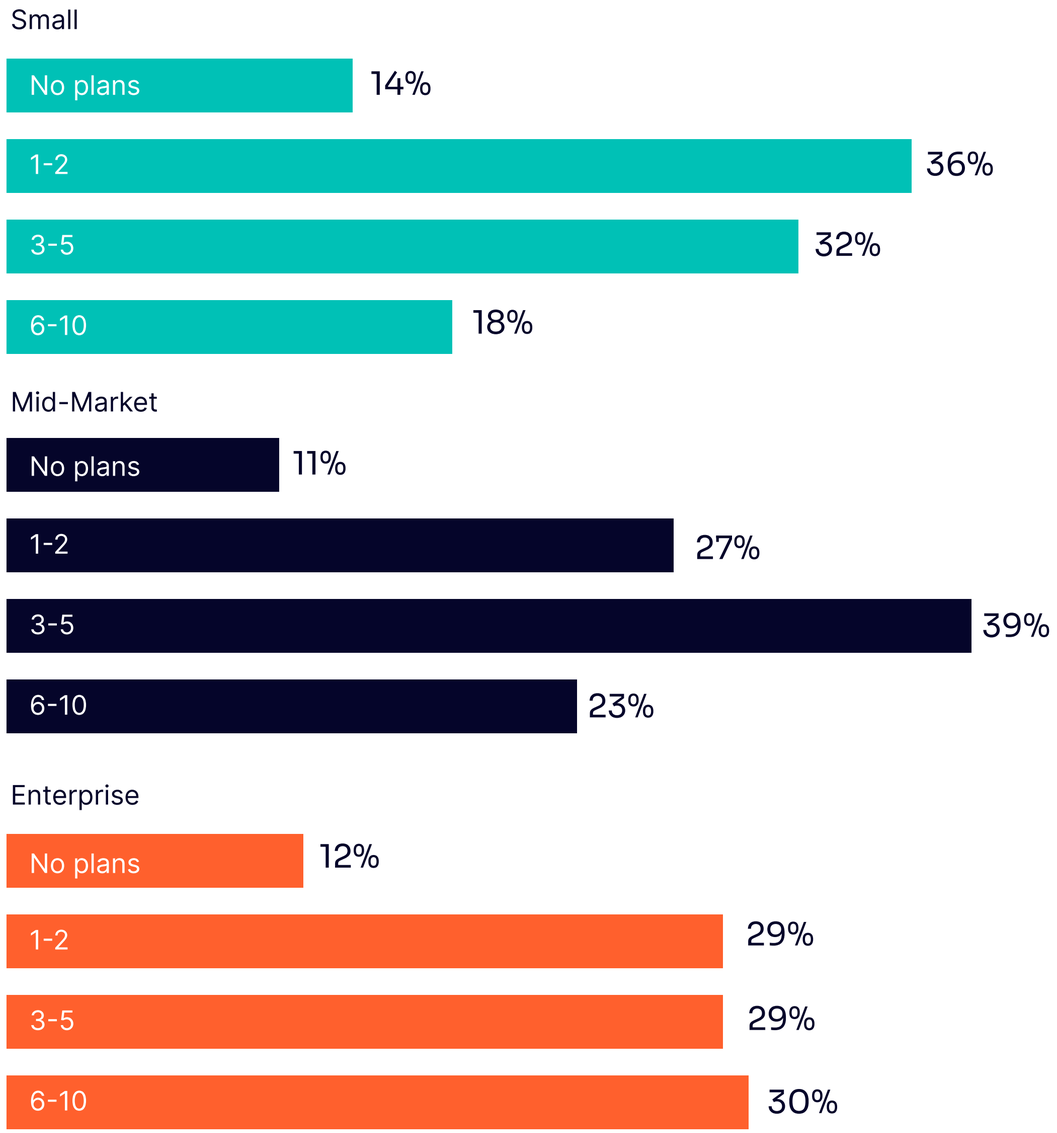
→ Efficiency depends on balancing people with automation and machine learning-driven fraud detection

We've found that the most effective teams use AI, automation and real-time monitoring to scale operations without increasing costs or headcount. These teams recognize that to support business expansion — whether entering new markets or launching new products — they can't rely solely on adding headcount to stay ahead.

88%

of Fraud Teams Report an Increase in Headcount as They Continue to Grow

→ Do you plan to increase headcount for your teams in the next 12 months? If so, how many new hires are expected?



Enterprise Companies Lead in Scaling Fraud Teams, With 30% Planning to Add 6-10 Team Members

Enterprise companies are making the biggest investments — over 59% are hiring more than 3 fraud professionals, signaling expansion and commitment to fraud prevention.

Mid-market organizations are scaling their fraud defenses, closely mirroring enterprise hiring patterns. Of these, 39% are hiring 3 to 5 team members.

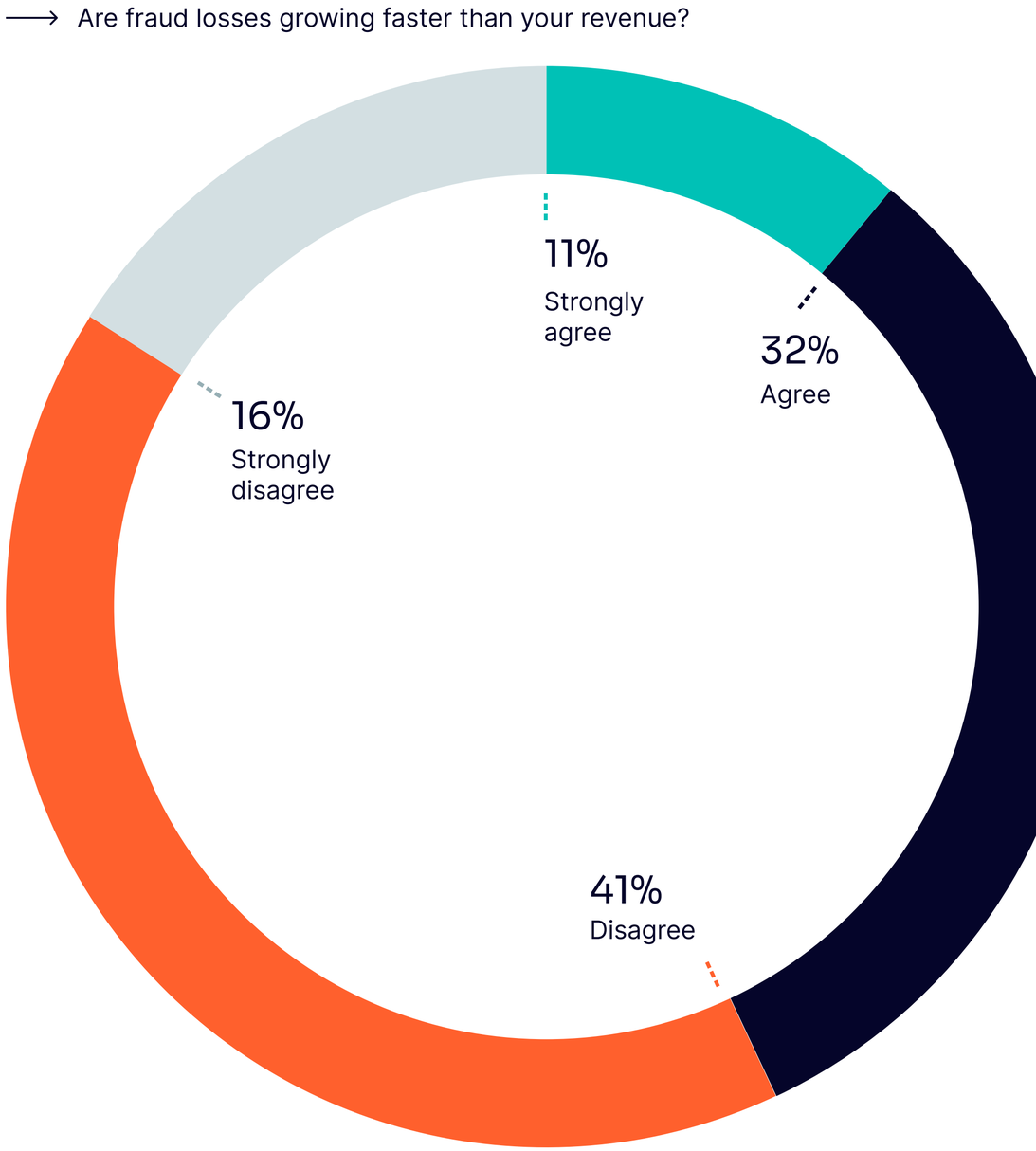
Small businesses recognize fraud's complexity, with 36% adding 1 to 2 people — an indicator of increasing awareness but more conservative hiring trends.

43% of Respondents Believe That Fraud is Growing Faster Than Revenue

For some, current fraud prevention efforts effectively mitigate losses, while for others, the rising sophistication of fraud schemes is placing pressure on margins.

The disparity highlights a nuanced reality and underscores the importance of tailoring fraud prevention strategies to match organizational risk profiles and scaling capabilities. Allocating the right resources can dictate success or further compound struggles.

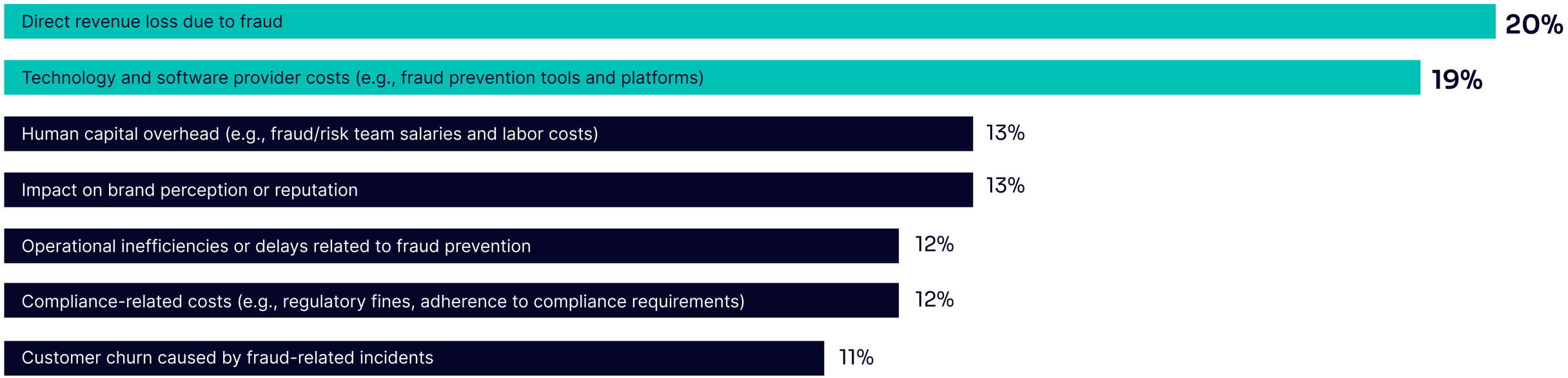
Adopting scalable, proactive measures will benefit businesses struggling to keep pace. Meanwhile, those managing fraud effectively must remain active and continue refining their approach to maintain balance as the risk landscape continues to change.



Direct Revenue Loss & Technology Spend: Leading Performance Indicators to Measure Program Success

Organizations often prioritize immediate financial metrics over operational inefficiencies and brand reputation, potentially underestimating the total impact of fraud.

⟶ What do you track to assess your organization's total fraud and risk management costs?



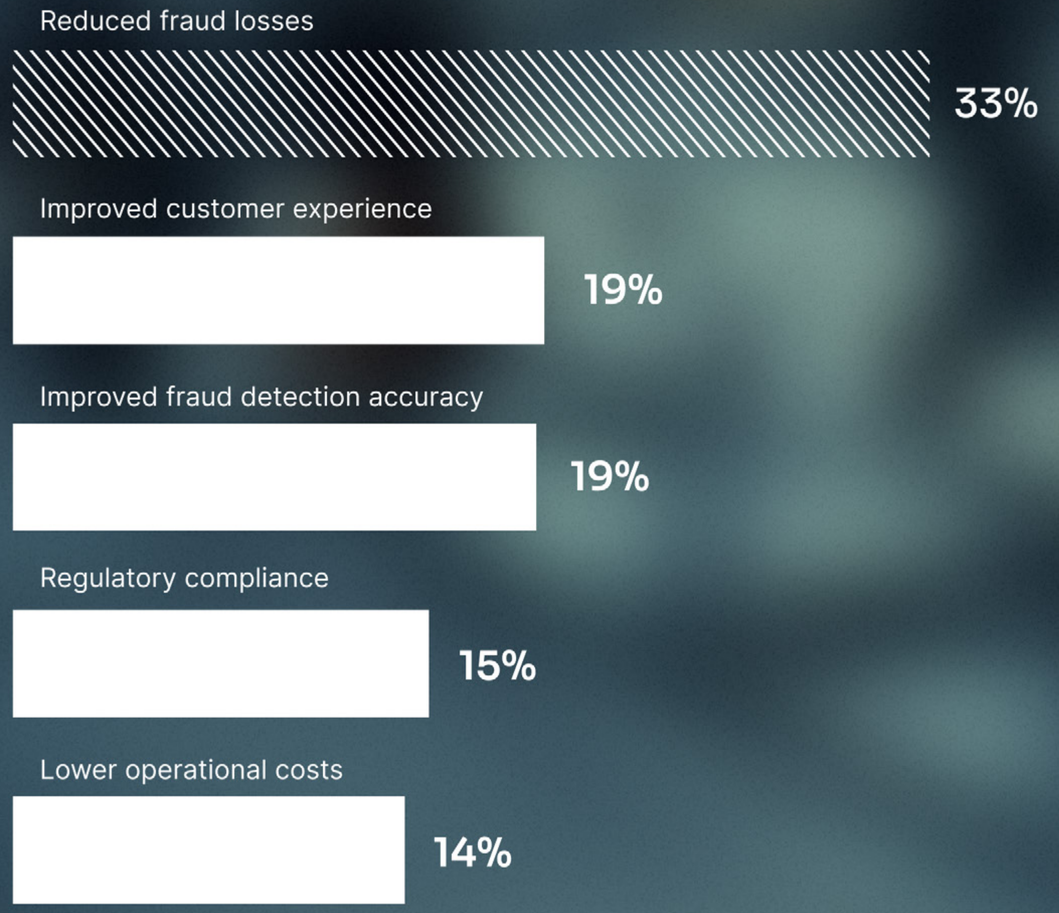
Showing Reduced Fraud Losses is the Strongest Indicator of ROI in Fraud Prevention

Like benchmarking standards, **33% of organizations overwhelmingly associate ROI with reduced fraud losses**. Secondary drivers include improved customer experience and increased fraud detection accuracy.

⟶ What percentage of teams surveyed prioritize customer experience?

60% of AML Compliance Teams **20%** of Risk Teams **18%** of Fraud Teams

⟶ What factors contribute the most to your perceived return on investment (ROI) in fraud prevention?



ROI Calculations Vary Across Different Industries

Financial Services

Financial services focus on direct fraud losses, compliance costs and operational risks while also accounting for long-term impacts like reputational damage and revenue loss.

Fintechs

Fintechs prioritize churn reduction, customer trust and tech-driven fraud mitigation, using real-time analytics to optimize fraud prevention and security without adding friction.

Payments

Payments measures fraud losses at the transaction level, emphasizing operational efficiency and fraud detection accuracy, to ensure secure and reliable transactions.

iGaming

iGaming tracks customer retention, chargeback rates and bonus abuse, with a focus on reducing fraud-related losses while improving player trust and engagement.

eCommerce

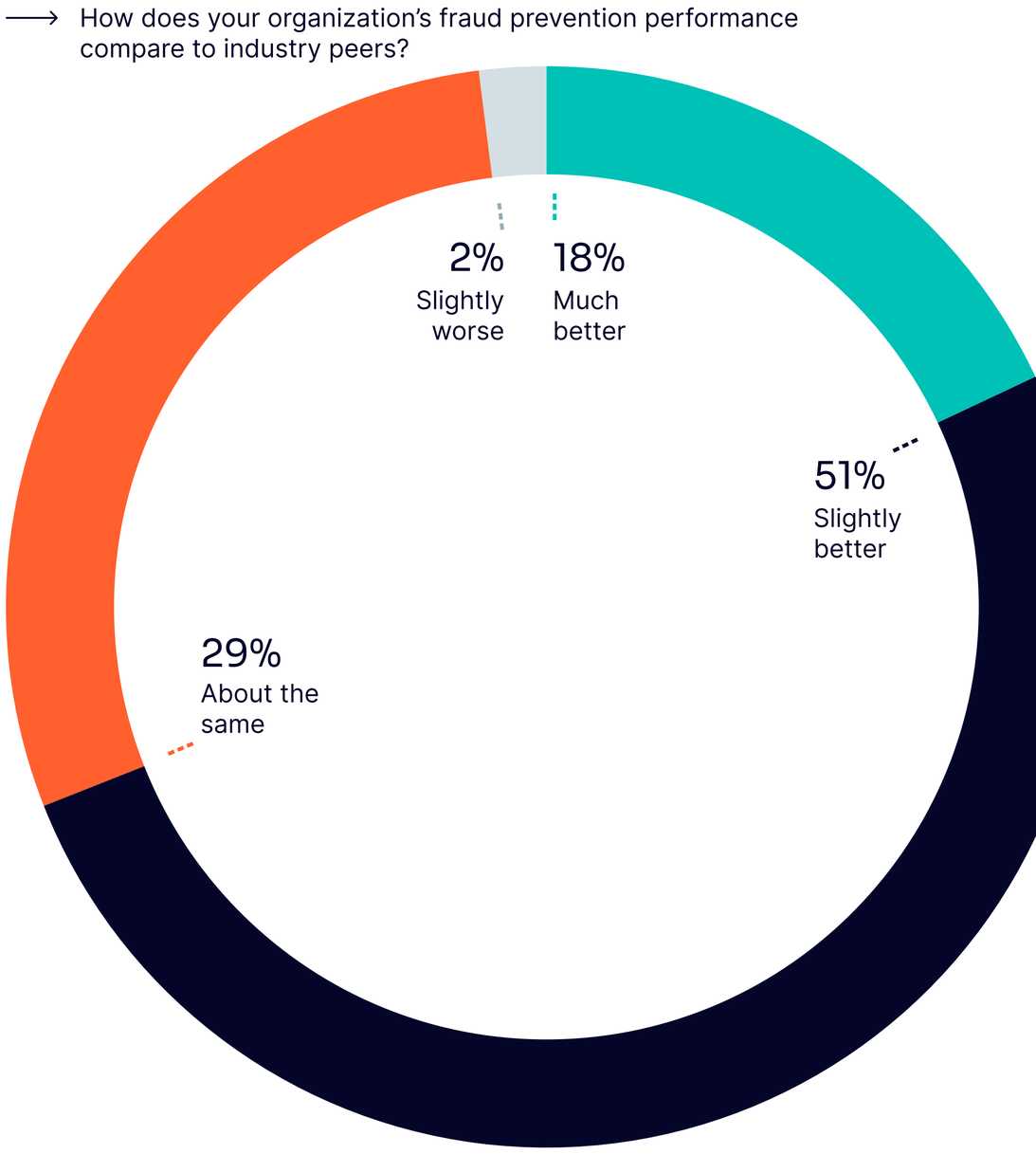
eCommerce balances efforts to reduce fraud losses from chargebacks, return fraud and inventory fraud while maintaining customer satisfaction rates to protect bottom lines.

69% Say They Outperform Peers, But Only 18% Think They Do Much Better

Most respondents believe they outperform peers in fraud prevention, with 18% claiming they perform ‘much better,’ reflecting growing confidence in fraud teams.

However, 29% say they perform ‘about the same,’ and others admit lagging, leaving room for innovation and adopting advanced tools and cross-team collaboration to get ahead.

iGaming respondents, in particular, expressed the highest confidence in outperforming their peers, while eCommerce respondents were likelier to feel they were simply meeting industry standards. This suggests that fraud challenges and prevention strategies vary across industries, with specific sectors taking more aggressive stances on fraud mitigation.



The Total Opportunity Cost of Fraud: Are You Measuring Every Metric?

The impact of fraud extends beyond direct financial losses, creating a ripple effect throughout your business. These hidden costs strain resources and slow growth, leaving organizations vulnerable to future threats.

Companies should consider using a 'Total Cost of Fraud' framework, measuring the following fraud-related categories:

Direct Losses
Fraud losses, technology costs, human capital costs

Operational Costs
Fraud analyst hours, manual reviews, investigation delays

Customer Impact
Lost lifetime value, churn due to false positives

Compliance Risks
AML fines, KYC process inefficiencies, regulatory violations

Percentages of Revenue spent on fraud

03

Successful Fraud Prevention = Right People + Right Technology

How Different Teams Contribute to Fraud Prevention

Fraud prevention is no longer just the responsibility of dedicated fraud teams. In today's interconnected business environment, fraud detection and mitigation require alignment across IT, finance, customer service to protect customers across every stage, from sign-up to ongoing account activity, reducing risks across the full lifecycle.

Successful fraud prevention requires the right people and technology — cross-team collaboration, AI-powered automation and scalable fraud strategies.

→ **IT & Security Teams** are fraud prevention power players, integrating fraud solutions with authentication, device intelligence and access management tools.

→ **Customer Service Teams** are frontline fraud detectors, identifying account takeover attempts and disputing fraud cases in real time.

→ **Finance & Payments Teams** are critical in chargeback management, risk analysis and balancing fraud prevention with revenue protection.

→ **Product & Marketing Teams** are building fraud-resistant user journeys, providing seamless yet secure onboarding experiences.

Successful Fraud Prevention Starts With IT & Security Team Collaboration

Our survey highlights how different company sizes prioritize collaborating with various departments to prevent fraud:

97% **IT & Security** consistently ranks as the most critical team across all company sizes

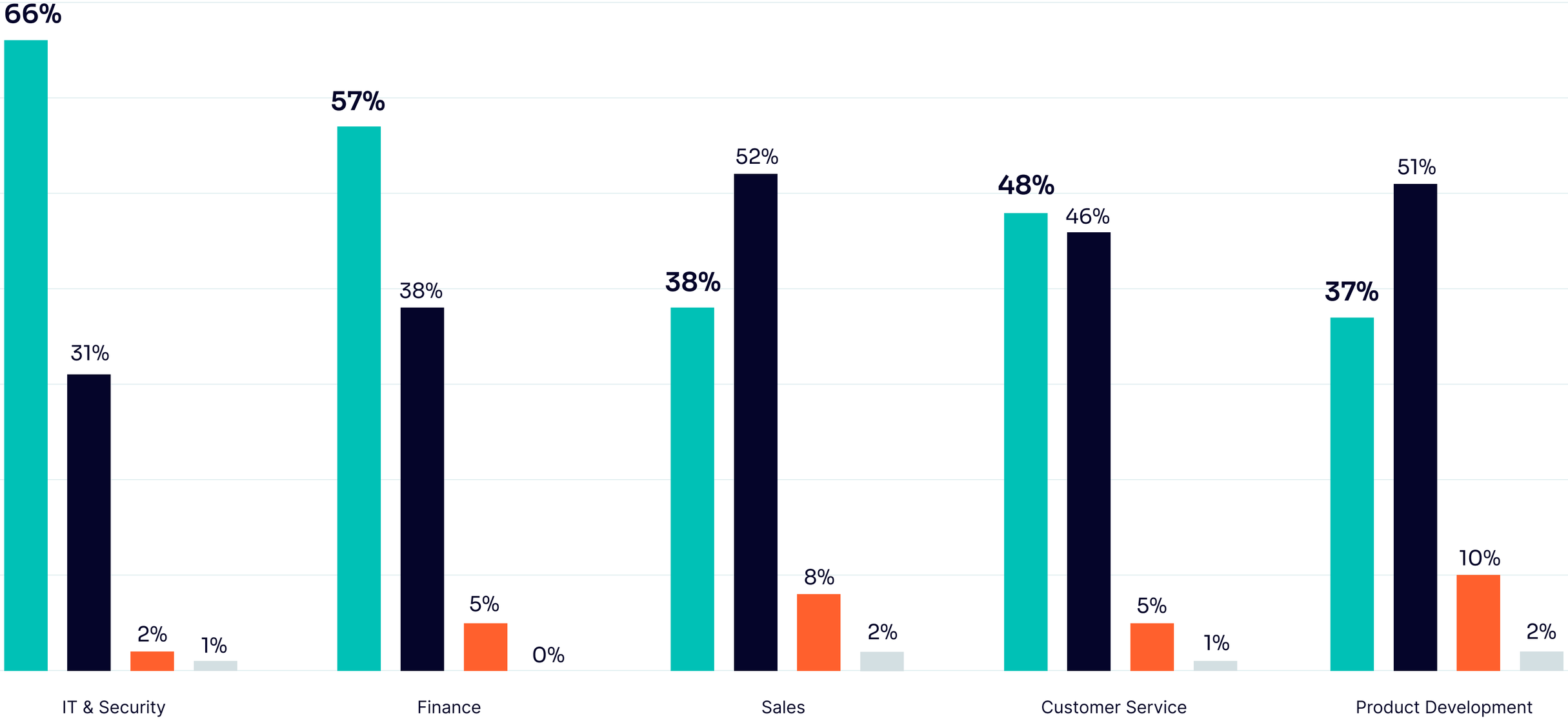
95% **Finance** follows closely in mid-market and enterprise companies

95% **Customer Service** holds greater importance in mid-market and enterprise companies compared to small businesses

89% **Sales** is labeled as a more critical function in enterprise organizations compared to small and mid-market businesses

89% **Product Development** is consistently rated as very important across the board, emphasizing the role of fraud prevention in product innovation

⟶ How important is it for your organization to collaborate with other teams to successfully prevent fraud?



95%

of Companies Are Cross-Training Teams to Handle Fraud Challenges — Is Yours?

As fraud grows in complexity, organizations can’t afford siloed knowledge.

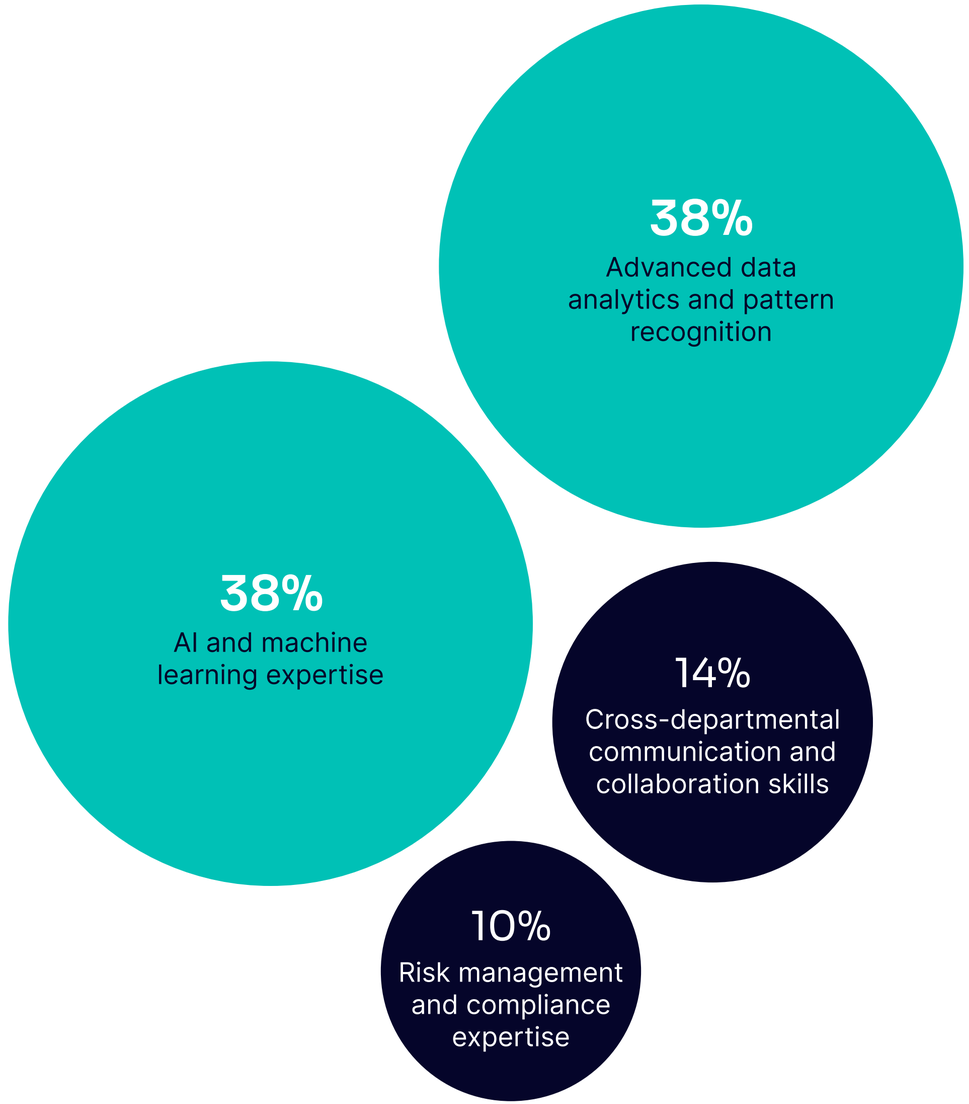
Our data shows that 95% have implemented or plan to implement cross-departmental fraud training for teams such as product, marketing and customer service to handle fraud challenges better.

Among the 5% that haven’t, most are mid-market (45%) and small businesses (38%), with enterprises making up only 17%.

76% of Most Sought After Fraud Prevention Skills Are AI & Data Analytics

Businesses need to close the fraud tech skills gap to keep pace with innovation. Our data shows that 76% of in-demand fraud prevention skills are related to advanced data analytics and AI and machine learning expertise.

⟶ What new skills or expertise do you anticipate needing the most in your fraud prevention team over the next 12 months?



04

AI Trends & Predictions

84% of Survey Respondents Believe AI Will Reduce the Need For Human Oversight

Fraud prevention is in a new era featuring AI as both the biggest threat and the most powerful tool. In 2025, fraud and risk teams must adapt to fight AI-driven fraud while leveraging AI for next-gen defense strategies.

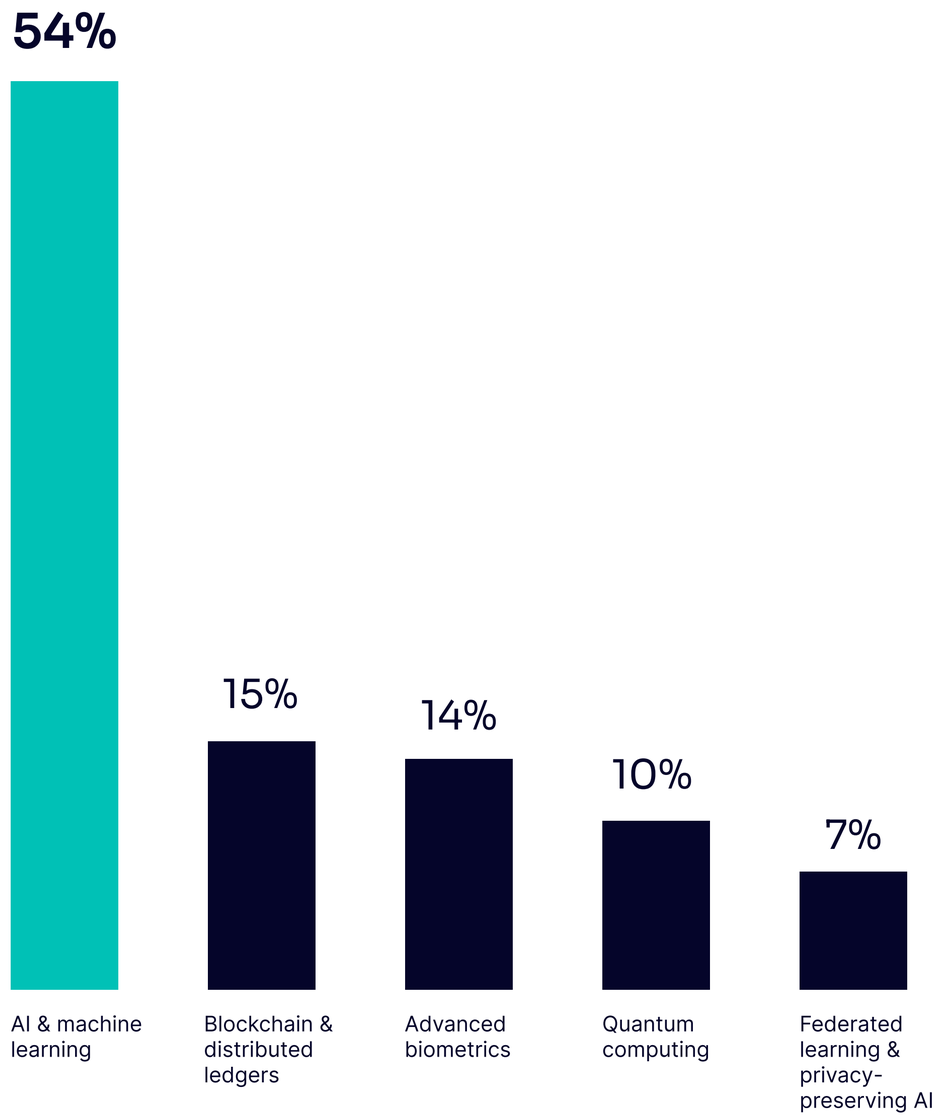
The AI-Human Balance
While AI delivers speed, efficiency and predictive capabilities, it also introduces risks: blindspots, overreliance and adversarial AI attacks.

Organizations must strike the right human-AI balance to maintain human intuition, contextual understanding and ethical oversight.

AI & Machine Learning Lead as Biggest Technology Impactors

AI and machine learning lead as the most transformative forces in fraud prevention. However, emerging technologies like blockchain and biometrics are quickly becoming essential, signaling a multi-layered approach to fraud defense.

⟶ What emerging technology do you believe will have the biggest impact on fraud prevention in the next 3 years?



83%

of Respondents Agree AI Will Reduce the Need for Manual Processes

Optimism around AI is high.
Most respondents view AI as a transformative tool for reducing manual processes in fraud detection. However, compared to its use in other industries, AI's role in fraud prevention is still quite nascent.

When fraud solution vendors tout their use of AI today, they most often refer to the subset of AI called blackbox machine learning. However, unlike transparent machine learning, this form of AI is isn't useful for regulators and the C-Suite, as it fails to provide a clear rationale for decision-making.

Other uses may include AI agents and AI-powered reporting assistance for compliance.

Top 5 Emerging Tactics Keeping Fraud Teams Up at Night

1

AI-Powered Fraud — Deepfakes, AI Phishing and Voice Cloning

2

Synthetic Identity Fraud

3

Account Takeover & Credential Stuffing

4

Social Engineering & Business Email Compromise

5

Exploitation of Instant Payments & Real-Time Transactions

Confidence in AI is High, But Skepticism Lingers

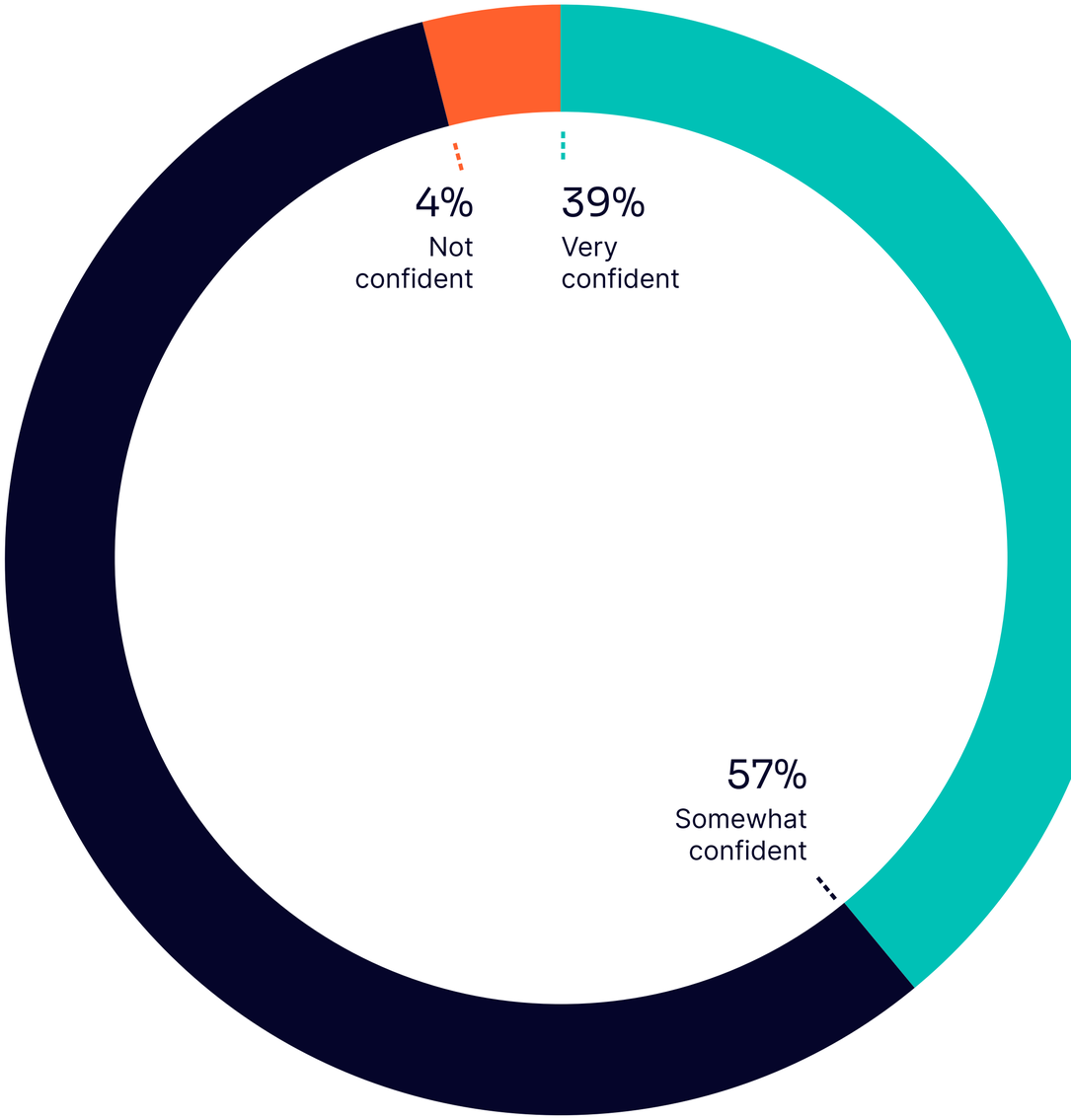
Of 574 respondents, **96% expressed confidence in AI tools** versus traditional fraud tools, but **57% reported hesitancy.**

Despite the high rate of accelerating AI-driven fraud, there remains skepticism about AI's ability to detect AI-generated fraud.

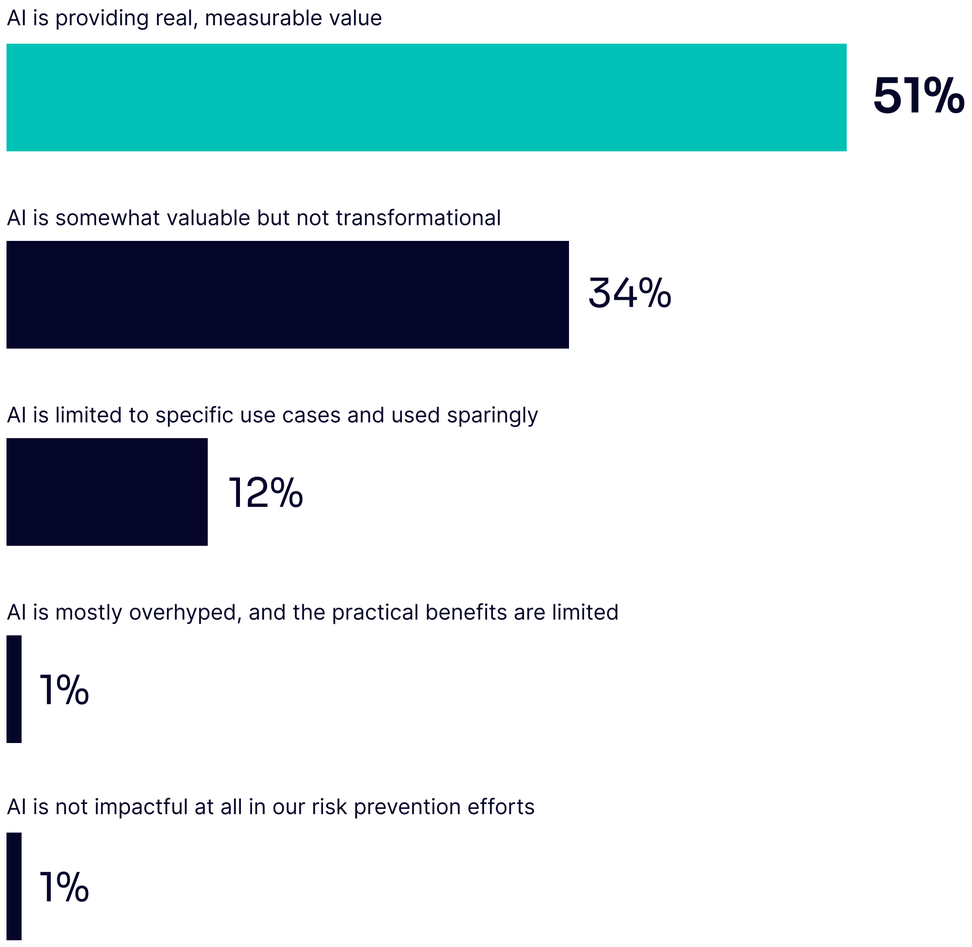
The challenge: how do we stay ahead?

Since fraudsters change tactics daily, organizations that rely on static rules risk falling behind. To stay ahead, organizations must leverage transparent AI insights alongside rule-based frameworks to ensure fraud decisions remain explainable, trustworthy and effective against evolving threats.

→ How confident are you in your current AI solutions versus traditional fraud tools in adapting to new challenges?



⟶ In your experience, are AI capabilities overpromised or does it provide real value to your fraud and risk investigations?



51% Are Finding AI Provides Real Measurable Value

Confidence in AI's value highlights the need for focused investments in training and new use cases.

As AI and ML adoption grows, organizations must also ensure they track measurable business impact — from fraud reduction to operational efficiencies — to solidify AI as a core part of their risk prevention strategy.

Service providers and industry leaders must collaborate to create practical use cases, starting with more minor quality-of-life improvements.

05

Despite AI Hype, Real-Time Transaction Monitoring Leads the Way

The Future of Fraud Prevention: Real-Time Transaction Monitoring

From instant bank transfers to blockchain-based transactions, real-time payment systems are reshaping how money moves — fast, borderless and, in many cases, irreversible.

Yet, fraud prevention systems are lagging, with many relying on outdated batch processing that analyzes data after the fact.

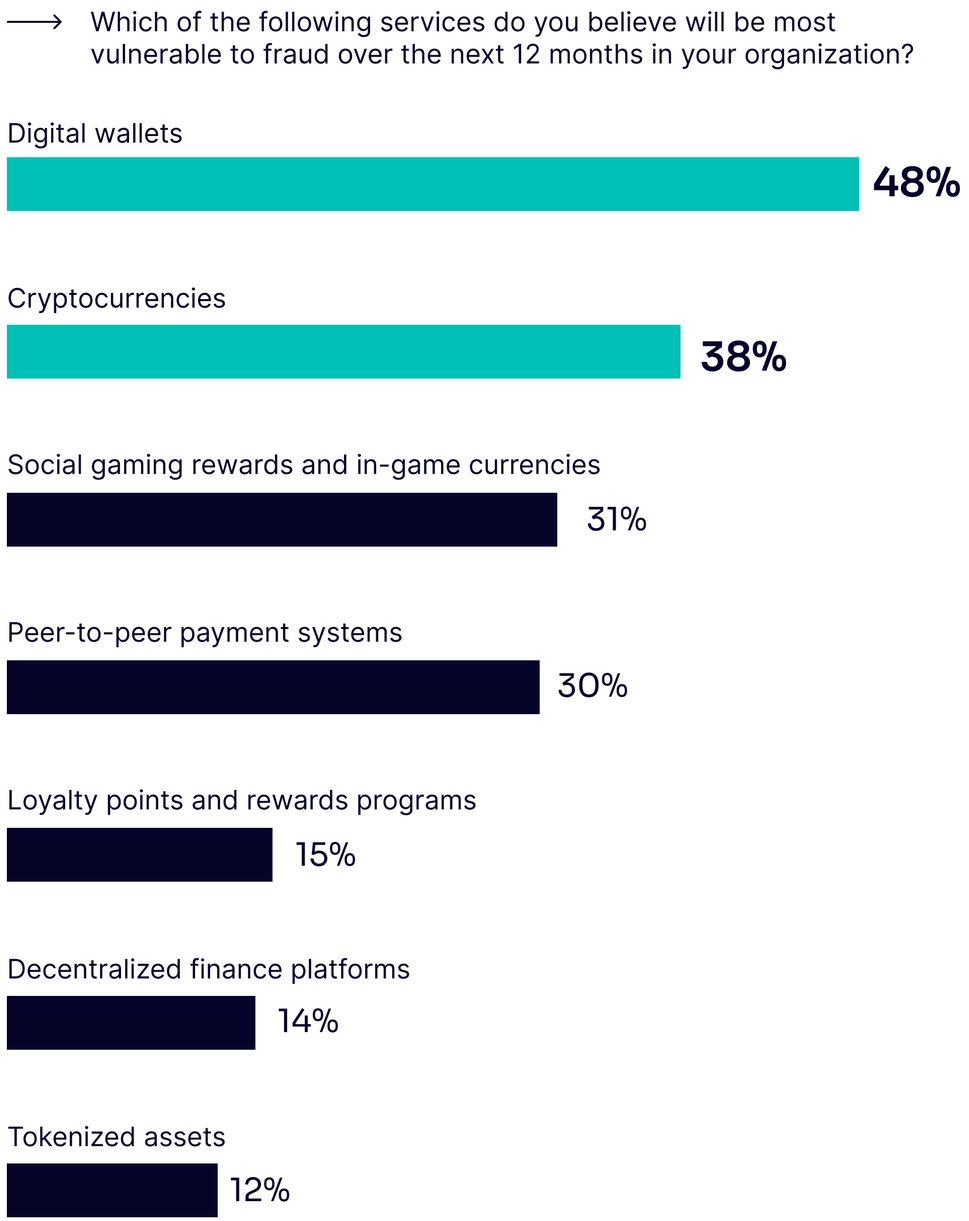
Survey respondents identified real-time transaction monitoring as the most essential fraud prevention investment for 2025, underscoring the demand for solutions that can detect and block fraud the moment it happens.

Fraud prevention solutions are evolving to support the rise of instantaneous payment networks, gaining popularity through policy changes and the crypto resurgence.

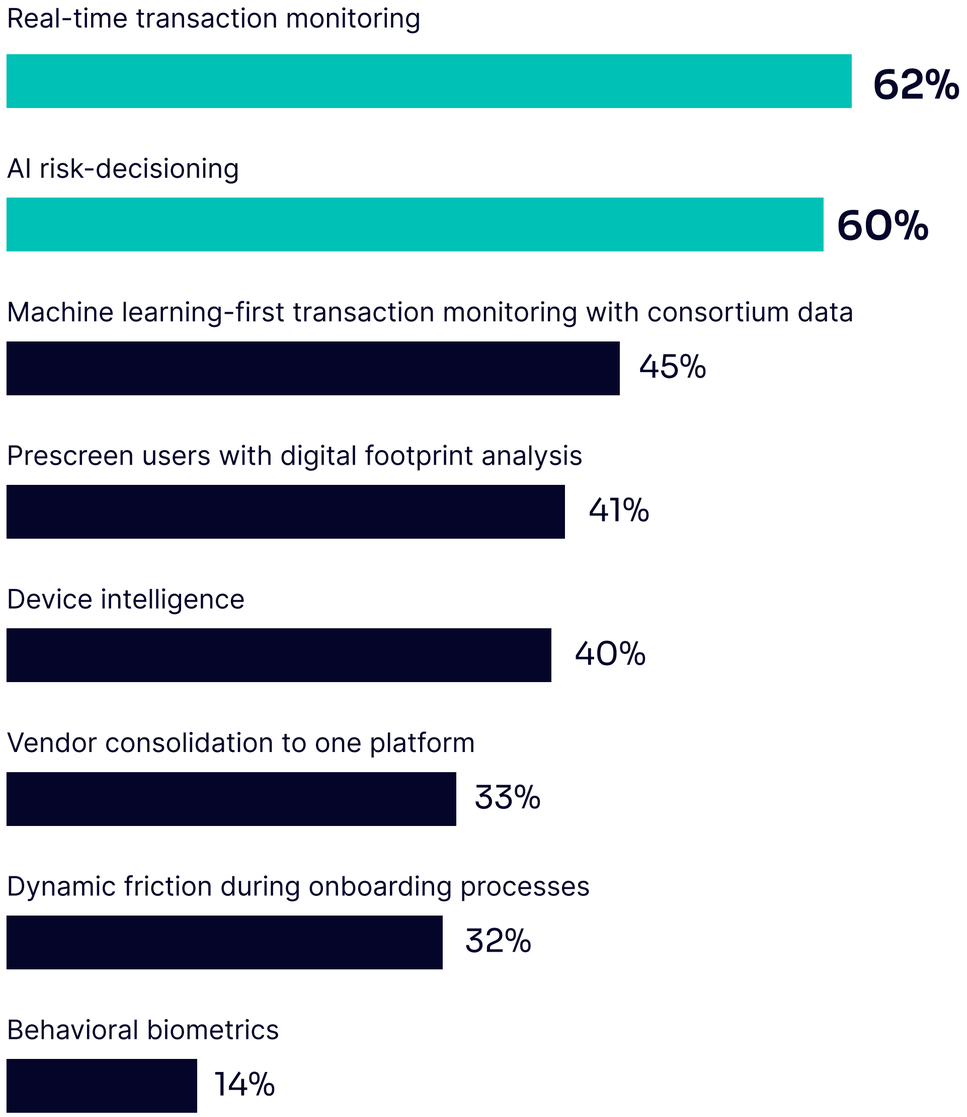
Such changes underscore the need for **real-time data in a centralized solution to improve AI risk decisioning and enable continuous transaction monitoring.**

Digital Wallets & Crypto Are Most Targeted Fraud Frontiers for 2025

Apart from the known fears around AI-generated threats, digital wallets and cryptocurrencies are the top fraud vulnerabilities for professionals right now.



→ Which of the following techniques do you believe will be the most effective component of your fraud prevention strategy over the next 12 months?



Fraud Teams Are Prioritizing Real-Time Transaction Monitoring & AI in the Next 12 Months

Real-time transaction monitoring is critical in our current instant payments environment, but some businesses need time to transition from batch processing.

By combining this form of monitoring with dynamic, transparent AI models, organizations can take a proactive approach to fraud prevention. A hybrid approach — leveraging AI for dynamic risk detection alongside rule-based logic — helps fraud teams achieve both speed and accuracy without losing control over decisioning.

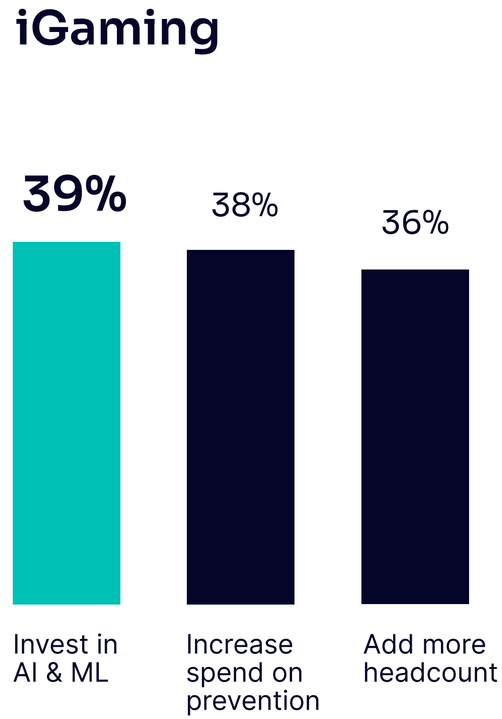
However, high-performing teams also recognize that fraud isn't limited to just transactions — it can occur at any stage of the customer journey. This is why they invest in real-time detection and decisioning across all touchpoints, ensuring threats are mitigated before they escalate.

Automation Plays Integral Role in Increasing Operational Efficiencies

Top priorities for 2025 include increasing investments in fraud and risk prevention technology. As AI rapidly expands its capabilities, the need to counteract AI has never been more crucial. Continual efforts to increase automation will help increase operational efficiencies and, in the long term, reduce costs.

Nearly 40% of Respondents Across Industries View AI & Machine Learning As Top Prevention Priority

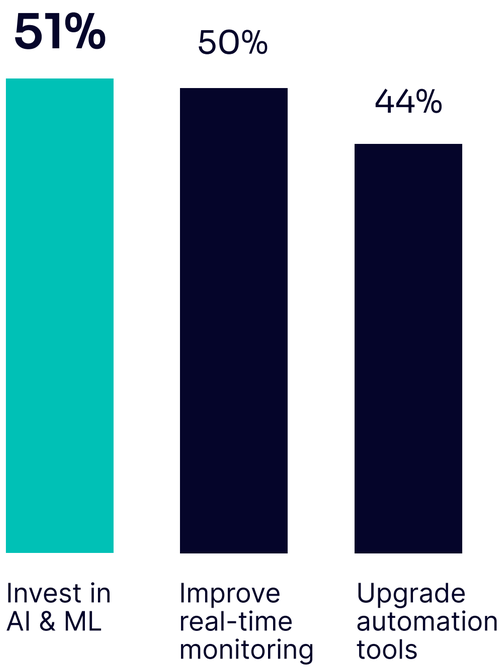
iGaming is the only sector expanding headcount, recognizing the need for human expertise alongside AI prevention.



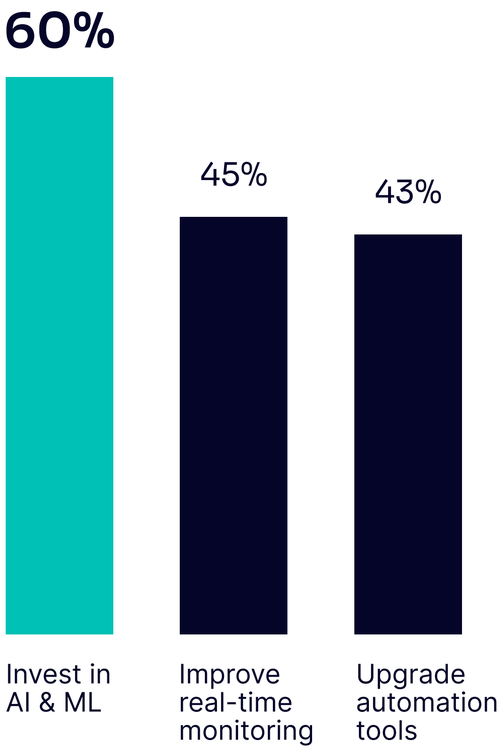
Payments and eCommerce prioritize real-time monitoring. With the rapid pace of digital transactions, these sectors emphasize faster fraud detection and response times to mitigate risk.

Financial Services, Fintech and iGaming all prioritize increasing spend on prevention tools to strengthen their fraud defenses ensuring that their technology and strategies remain ahead of evolving threats

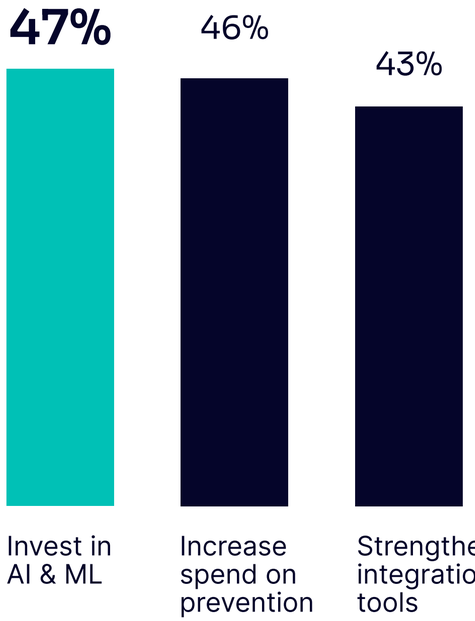
Payments



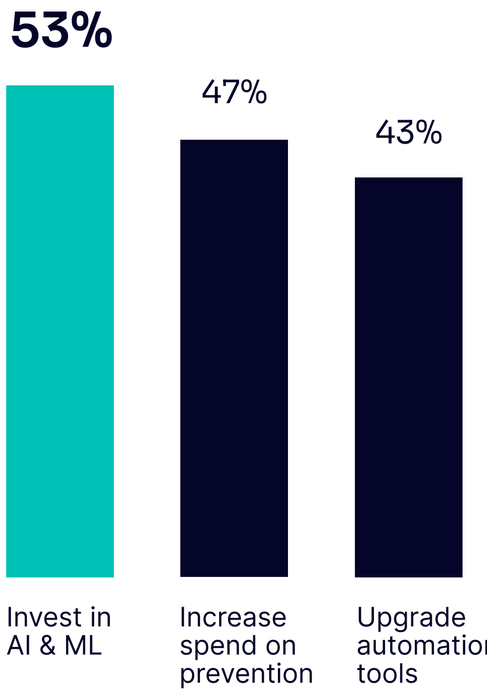
eCommerce



Financial Services



Fintech



06

Final Takeaways

1 Fraud Budgets & Teams Are Growing – But Tech Investments Must Be Real-Time & Scalable

To maximize ROI, investments must prioritize real-time monitoring, AI-driven automation and advanced analytics to reduce manual workloads and improve detection speed — while maintaining essential human oversight.

2 The Total Cost of Fraud Goes Beyond Direct Losses

Fraud's hidden costs — ranging from operational expenditures and inefficiencies, compliance fines and customer churn — create a ripple effect across the business. Organizations that fail to account for the total cost of fraud may underestimate its true impact, leaving them vulnerable to long-term financial and reputational risks.

3 Real-Time Transaction Monitoring is the #1 Investment Priority

Businesses are shifting from outdated batch-based transaction monitoring to real-time transaction monitoring, ensuring they can stop fraud before it happens.

4 Collaboration & Cross-Team Intelligence is a Competitive Advantage

While IT and security teams are essential to help tackle fraud prevention challenges, it's equally important to train teams across departments on how to spot fraud challenges.

5 Unlocking Autonomous AI Is Contingent On Centralized, Real-Time Data

Organizations are struggling with limited AI use cases and fragmented data. Moving closer to autonomous AI-driven fraud prevention will require centralized, real-time data and transparent risk decisioning.

6 AI & Data Analytics Are the Two Most Sought After Fraud Prevention Skills

Organizations are prioritizing skills related to AI and advanced data analytics to enhance detection accuracy and automate risk decisions.

The SEON Perspective: On The Road to Autonomous Fraud Prevention — Where Are We Now?

Throughout this report, we examine the transformation of fraud prevention from traditional manual methods, such as static rules, to autonomous AI-driven risk decisioning.

While AI significantly enhances fraud detection capabilities, it still faces challenges with complex fraud schemes that require nuanced, contextual understanding — areas where human analysts excel. The current ideal fraud prevention model marries AI efficiencies with human insight, not replacing but augmenting human oversight.

Looking ahead, fraud prevention will develop into a predictive, self-learning system where AI tackles the real-time monitoring of vast transaction volumes and dynamically adapts to emerging threats. Despite the push toward automation, complete autonomy in fraud prevention will require the need for centralized, real-time data to feed AI models. This data format will enable AI to consistently improve risk predictions and adapt security measures dynamically, thereby enhancing the accuracy and responsiveness of fraud prevention systems.

As we continue on this path, the intersection of innovative AI applications and expert human intervention will further refine and define the future of fraud prevention at SEON and beyond.

SEON

Stop Fraud Before It Happens

This report is based on insights from a survey commissioned by SEON, gathering perspectives from fraud prevention professionals across industries. Research and analysis were conducted by Christina Brichetto & Katy Chrisler.

Read more at seon.io

The Total Opportunity Cost of Fraud is Bigger Than You Think

Read the Article ⟶

Leveraging AI & Innovative Tech to Combat Emerging Complex Fraud Schemes

Read the Article ⟶

Traditional Fraud Prevention Measures Aren’t Enough

Read the Article ⟶