Navigating the Future of Secure iGaming

A vertical excerpt of the 2025 Digital Fraud Outlook

Table of Contents

Introduction

The iGaming industry stands at a critical crossroads. While the sector continues its remarkable growth trajectory — projected to surpass $107.70 billion this year[1] — it simultaneously battles increasingly sophisticated fraud tactics that threaten to undermine profitability, player trust and regulatory compliance.

As the digital economy and its offerings evolve, so too do fraudsters' tactics. Operators must transform their approach to fraud prevention from a cost center into a strategic competitive advantage. Proactive strategies combining real-time transaction monitoring, AI innovation and human expertise have become the hallmark of resilient platforms.

Our 2025 Digital Fraud Outlook report surveyed 574 senior fraud, risk and compliance professionals across geographic regions — with 130 respondents from iGaming companies — to compile insights into how operators are prioritizing fraud prevention budgets to invest in technologies and teams to combat fraud more effectively.

1 Statista: Gambling Worldwide Market Insights

Key Industry Trends

The following key industry trends highlight exactly where operators are investing and what they are doing to adapt to the increasingly sophisticated threat landscape:

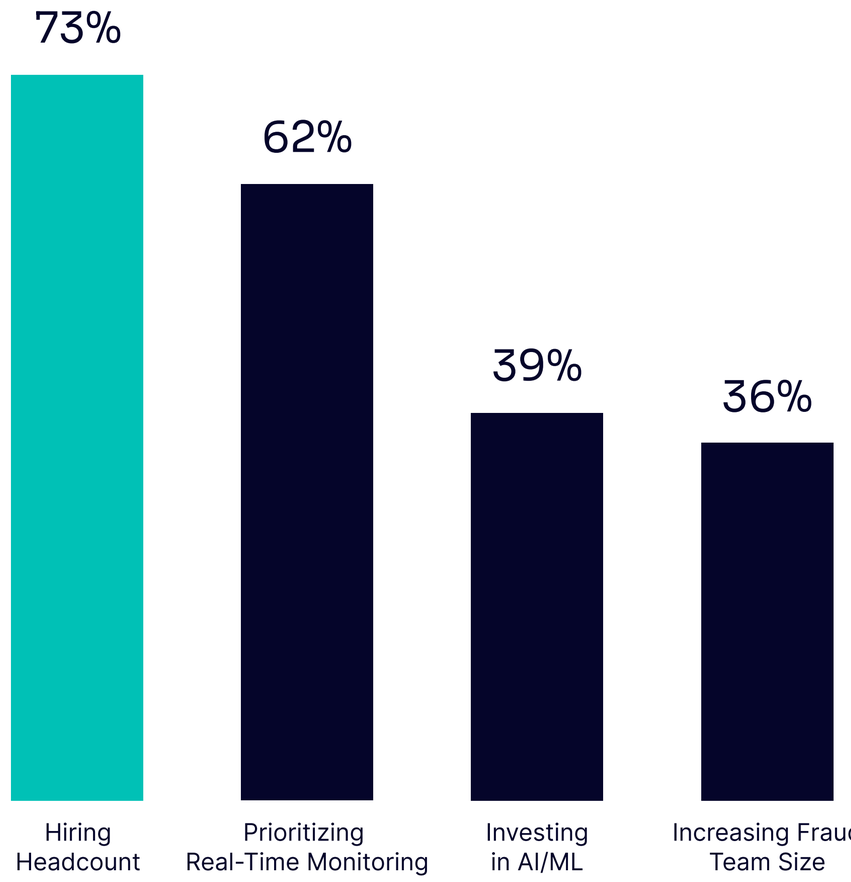
→ **Top concerns: Chargeback & bonus abuse**
Unlike other industries which focus on transaction fraud, iGaming operators prioritize mitigating chargeback rates and fraudulent behaviors like multi-accounting and bonus abuse.

→ **Operators are increasing fraud prevention investments**
73% of iGaming companies plan to increase fraud prevention headcount by at least 3-5 hires in the next 12 months, reflecting the sector's emphasis on operational resilience and willingness to spend not just on technology but also on human expertise.

→ **Real-time transaction monitoring is the #1 investment priority**
62% of organizations now favor real-time transaction monitoring over batch-based or other traditional fraud detection methods, enabling instant detection and response abilities to stop fraud before it impacts revenue.

→ **AI and machine learning are essential tools, but human expertise remains critical**
39% of iGaming companies plan to invest in AI and machine learning, 38% anticipate increasing spending on fraud prevention and 36% will increase fraud team headcounts within the next 12 months.

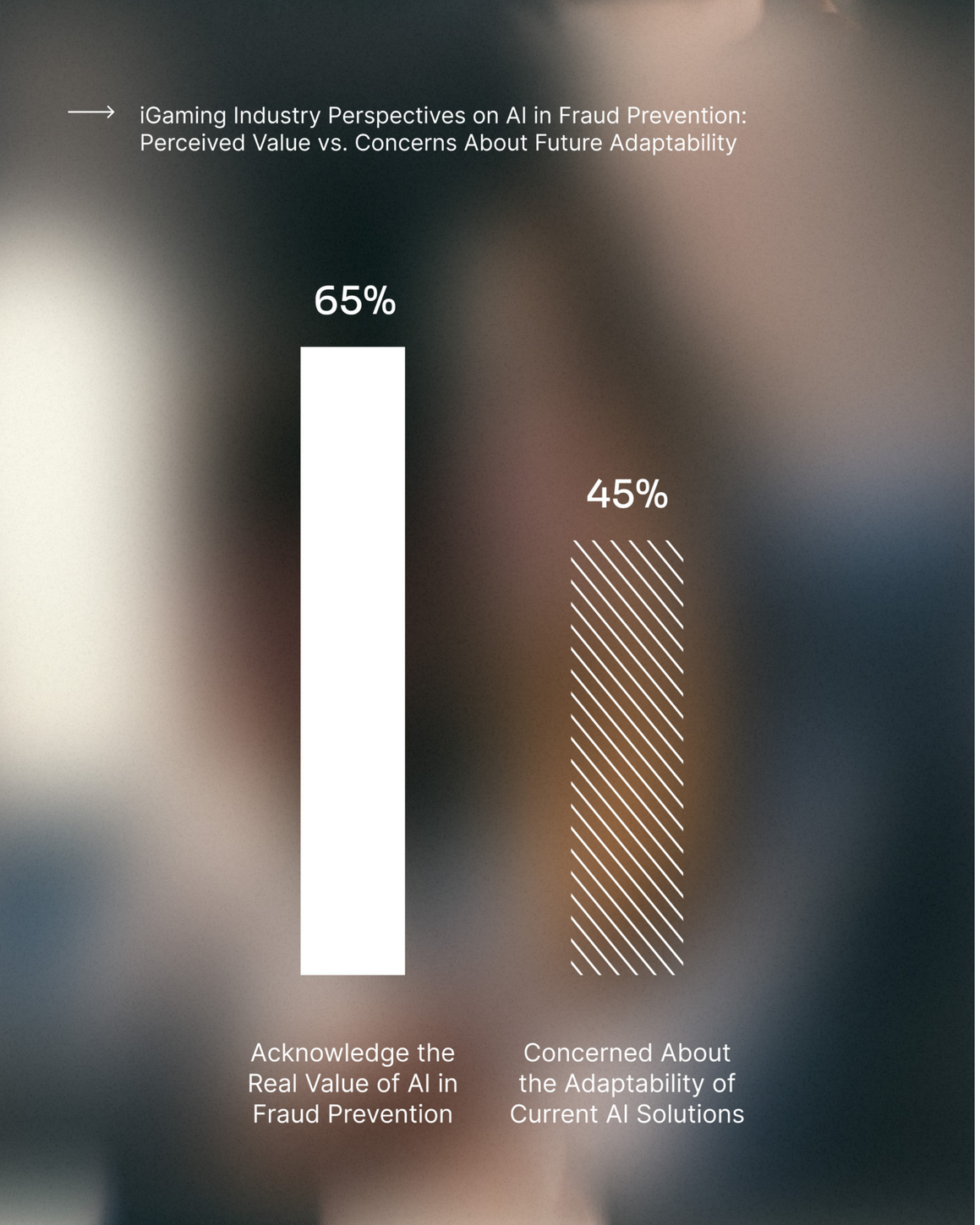
→ The percentage of companies investing in each area:



How iGaming Differs From Other Sectors

In most industries, fraud prevention is a quiet, behind-the-scenes safeguard — a way to avoid losses and stay compliant. But in iGaming, it sits at the center of the business model. The stakes are higher, the fraud tactics are more creative and the margin for error is razor-thin. To succeed, operators need to think beyond basic fraud controls and address challenges uniquely tied to player behavior, platform integrity and long-term trust.

What sets iGaming apart?
Let’s start with the financial impact: fraud prevention doesn’t just protect the bottom line — it actively fuels it. This dynamic leads to a different set of priorities, including a focus on behavioral analytics, battles against synthetic identities and stolen credentials and an understanding that player trust is a competitive asset, not just a nice-to-have.



Here’s where those differences stand out most:

→ **Fraud prevention is revenue-critical**
In payments and eCommerce, fraud prevention is often a compliance and cost-mitigation function. In iGaming, it directly impacts profitability due to its effect on player trust and retention.

→ **Higher reliance on behavioral authentication**
While financial services prioritize KYC and AML compliance, iGaming fraud teams emphasize tracking behavioral anomalies, gaming patterns and betting habits. Fifty-two percent of iGaming companies use behavioral biometrics to detect suspicious activity.

→ **Greater exposure to synthetic identities & stolen credentials**
Fraudsters frequently exploit gaming platforms using fake identities, collusion tactics and stolen payment details. 65% of iGaming respondents agree that AI provides real value in fraud prevention, but 45% have concerned about the adaptability of current AI solutions and acknowledge the real value of AI in fraud prevention.

→ **Player trust is a competitive advantage**
Unlike fintech or payments organizations, fraud prevention efforts significantly influence player retention in iGaming. A single bad experience — such as wrongful account suspension or disputed winnings — can push players to competitor platforms.

Emerging Fraud Threats Reshaping the iGaming Realm

As iGaming platforms evolve to offer faster payouts and smoother user experiences, fraudsters are evolving just as quickly — sometimes faster. Features designed to attract and retain players are now weaponized against operators. Traditional fraud detection methods struggle to keep pace with attacks that are speedier, smarter and more sophisticated.

What's fueling this new wave of threats? It starts with scale and automation. Fraudsters are no longer lone actors: they're using bots, AI and stolen data to exploit platforms, from bonus abuse to account takeovers (ATO) systematically. The rise of real-time transactions only accelerates the problem, leaving operators less time to react and at a greater risk of loss.

Here are the tactics fraud teams are scrambling to get ahead of:

1 Weaponized Bonuses and Identity Farms

Fraudsters aren't just creating a few fake accounts — they're running large-scale identity farms fueled by synthetic profiles and stolen credentials to drain welcome offers, loyalty rewards and VIP perks with industrial efficiency.

2 AI-Powered Deception at Scale

Deepfakes and AI-generated identities are no longer future threats — they're actively undermining authentication processes, with fraud teams now battling audio impersonation, manipulated documents and bots that can mimic player behavior in real time.

3 Real-Time Fraud in an Instant-Payout World

Instant withdrawals and lightning-fast payments are raising the stakes. Fraudsters exploit speed, slipping through static detection models before any manual review is possible — forcing operators to rethink their entire approach to real-time risk.

4 The Chargeback Economy

Friendly fraud has evolved into a calculated tactic rather than a one-off occurrence. Fraud rings work together to abuse chargebacks, using stolen payment methods to place bets and later reversing charges — effectively turning payment disputes into profit. Another growing threat is third-party fraud related to chargebacks. In these cases, fraudsters hijack user accounts, drain funds to a paycard or wager them, and the legitimate user later disputes the transaction. The operator is hit twice: first losing the stolen funds and then being forced to reimburse the player's claimed losses.

5 Automated Account Takeovers

Credential stuffing attacks have advanced well beyond brute-force attempts. Modern bots adapt and evolve, using stolen credentials and behavioral mimicry to blend in, hijack accounts, and quickly move money to external pay cards or gamble it away. The fallout doesn't stop there — users report these thefts as unauthorized transactions, triggering chargebacks. Operators end up on the hook for both the stolen funds and player reimbursements, making account takeovers a double-edged threat that skews gameplay outcomes and drains revenue.

The iGaming Fraud Narrative: What the Data Tells Us

The story emerging from the data is one of evolution and urgency. iGaming operators are no longer content with reactive fraud detection; they're building proactive, multi-layered defenses designed to keep pace with increasingly complex threats. The traditional "detect and respond" model gives way to continuous monitoring and predictive intervention.

Real-time transaction monitoring has become table stakes. Batch-based detection is already obsolete in a space where bets are placed and payouts processed in seconds. Fraud teams are leaning into real-time analytics to catch anomalies as they happen and before they translate into losses or damage player trust.

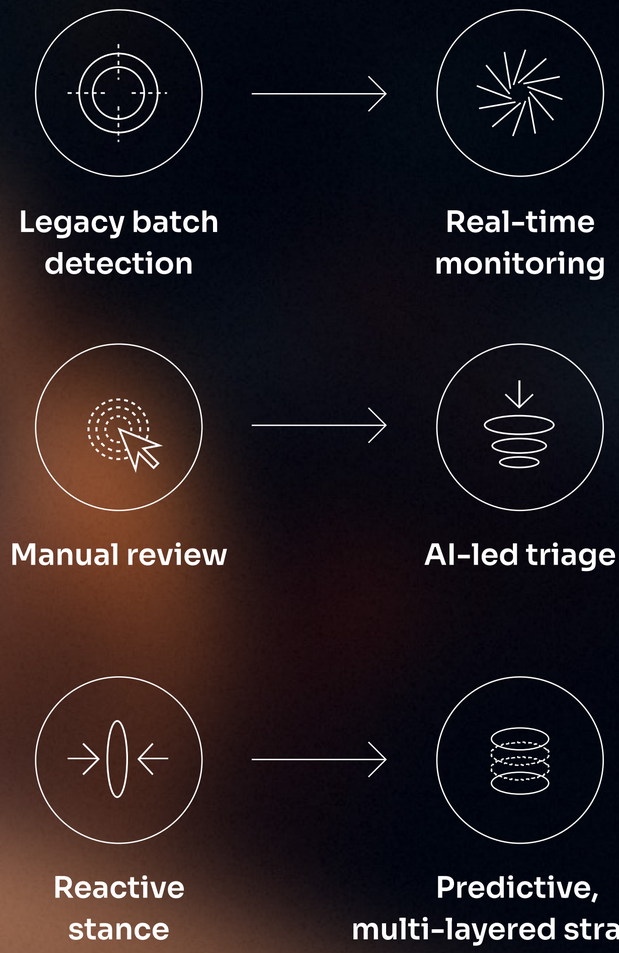
90%

of iGaming companies believe AI will drastically reduce the need for manual investigation, freeing up teams to focus on strategy.

AI sits at the heart of this transformation, offering both promise and pressure. **An overwhelming 90% of iGaming companies believe AI will drastically reduce the need for manual investigation, freeing up teams to focus on strategy.** But this optimism is tempered by reality: nearly half of respondents report fraud losses outpacing revenue growth. This disconnect signals a clear takeaway: while AI is part of the answer, its deployment needs smarter investment, better tuning and constant refinement.

The message is clear: fraud tactics are scaling in sophistication, automation and speed. Prevention strategies must evolve at the same pace, or operators risk losing not just money but the trust and loyalty of their player base.

How Fraud Tactics Are Changing



What iGaming Operators Must Do Next:

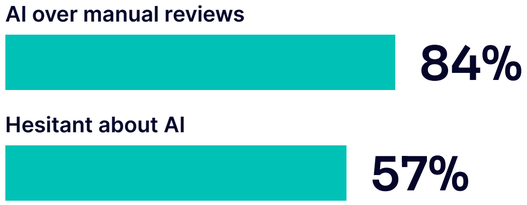
Turning fraud into a competitive advantage in iGaming, fraud prevention isn’t a back-office function — it’s a strategic advantage. The operators pulling ahead treat it as core to player experience, brand reputation and revenue growth. The data signals a clear direction: fraud teams can’t simply react — they must anticipate, adapt and outpace. Here’s what the smartest operators are prioritizing right now:

Move at the Speed of the Player

Instant transactions demand instant decisions. The industry consensus is clear: 56% of iGaming companies rate real-time transaction monitoring as the most effective defense. If fraud detection lags behind player activity, the damage is already done. Real-time risk scoring is now the baseline.

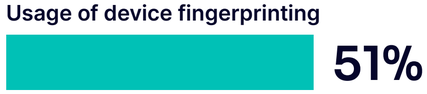
Trust AI, but Verify

AI is the engine powering faster, smarter fraud detection, but it's not a set-and-forget tool. While 84% of fraud teams believe AI will reduce reliance on manual reviews, nearly half still worry that fraud losses are growing faster than revenue. And with 57% hesitant about AI's resilience against AI-generated fraud, human expertise remains critical. The winning approach? Combine machine intelligence with human judgment to fine-tune detection without alienating legitimate players.



Watch Patterns, Not Just Transactions

Fraud doesn't always show up in a single suspicious payment. Often, it's a subtle pattern across devices, login habits and user behavior. 51% of operators already rely on device fingerprinting to spot bots and multi-account abuse. However, the next step is investing in deeper behavioral analytics and digital footprint analysis, turning fragmented signals into actionable intelligence.



Make Fraud Prevention Part of the Player Promise

Players want seamless gameplay, fairness, security and confidence that the platform has their back. Measuring fraud prevention ROI isn't just about reducing losses; it's about retention. 35% of operators cite reduced fraud as the top measure of success, followed by (20%) lower operational costs and (16%) better player experiences. The operators prioritizing trust will keep players loyal long after the bonuses run out.

Top 3 Takeaways for iGaming Fraud Prevention

The data makes one thing clear: iGaming fraud prevention is no longer a technical challenge — it's a strategic differentiator.

Operators who view it as a balance between protection and player experience are already positioning themselves ahead of the market. But with threats becoming more complex and player expectations rising, knowing where to focus next is critical.

Here are the three most important priorities for operators looking to turn fraud prevention into a competitive advantage:

1

Confront Third-Party Fraud at Scale

ATOs and chargeback abuse aren't occasional headaches — they're systemic threats. Fraudsters run large-scale credential-stuffing attacks, exploit real-time payouts and leverage chargebacks as a revenue channel. Left unchecked, this not only drains profits but damages the platform's reputation and player trust. The solution requires layered defenses: advanced device intelligence and real-time monitoring to detect and stop fraudulent behavior before it escalates.

2

Invest in Behavioral Biometrics to Separate Good Players from Bad Actors

Fraudsters can spoof identities and manipulate documents, but they can't replicate human behavior. That's why 52% of iGaming operators now consider behavioral biometrics one of their most effective tools. Tracking subtle markers — from mouse movements and typing patterns to gameplay rhythms — allows operators to detect fraud without adding friction. This can result in faster approvals for genuine players and automatic red flags for suspicious activity, all happening behind the scenes.

3

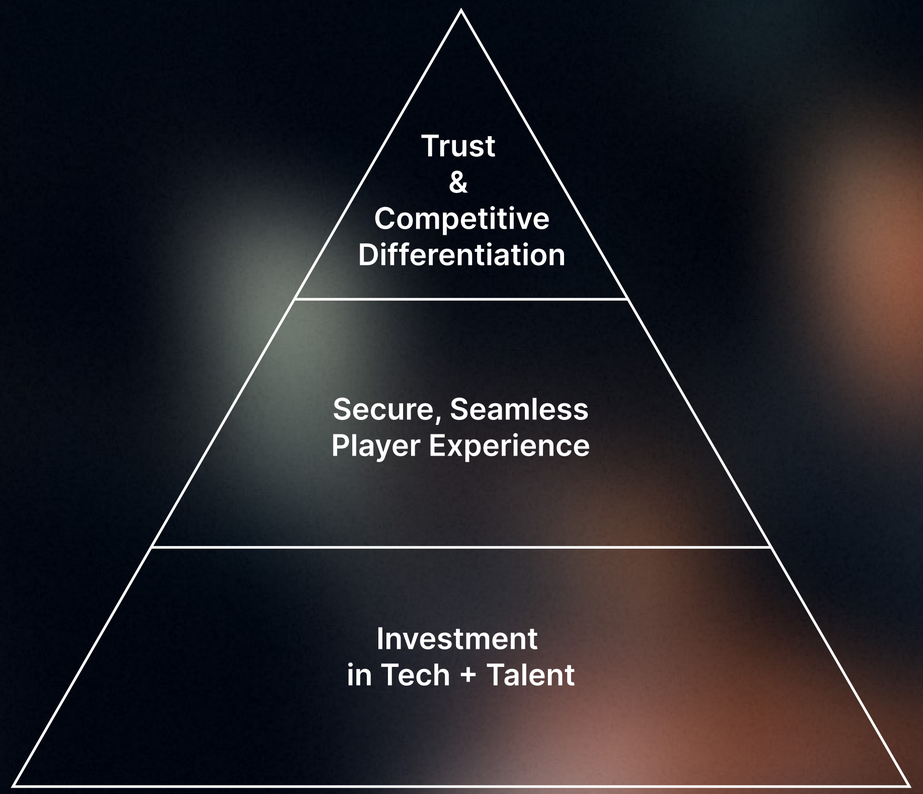
Make Frictionless Fraud Prevention Part of Your Brand Promise

In iGaming, trust is fragile, and false declines or delayed payouts can drive players straight to competitors. The best operators have realized that security must feel invisible. Real-time detection, AI-based risk scoring and behavioral analytics now form the backbone of a seamless player experience. Those who get it right not only protect revenue but also build loyalty and lifetime player value.

A New Era of Investment, Innovation & Trust

As iGaming continues its rapid growth, the battle against increasingly sophisticated fraud has become a defining challenge — and a defining opportunity. Operators who treat fraud prevention as a strategic lever, rather than a cost center, are positioning themselves to lead. The data is clear: those who invest in advanced technologies, real-time monitoring, behavioral analytics and human expertise can reduce fraud while strengthening player trust and loyalty.

In this new era, winning goes beyond stopping fraudsters. It's about delivering a secure, frictionless player experience that fuels retention, drives revenue and builds long-term competitive advantage. The operators who strike this balance — using intelligent tools without losing sight of the human element — will set the standard for the industry. In a market where players can switch platforms in an instant, security that protects without intruding has become imperative for business. Those who get it right won't just keep pace with the future of iGaming — they'll define it.



Want the Bigger Picture?

The iGaming sector isn't alone — across industries, fraud is scaling in speed, complexity and impact. In the full **2025 Digital Fraud Outlook**, we break down insights from 574 fraud, risk, and compliance leaders in Financial Services, Fintech, Payments, eCommerce and iGaming.

See how top organizations are building smarter defenses, investing in AI-driven solutions and moving at the speed of fraud. Explore the full report to benchmark your strategy, anticipate emerging threats and lead your team into the future of fraud prevention.

Read the full report now ⟶

SEON

About SEON

SEON helps top-tier risk teams detect and stop fraud and money laundering. By combining real-time digital footprint analysis, device intelligence and AI-driven rules, SEON empowers over 5,000 businesses globally to prevent threats before they occur. SEON operates in Austin, London, Budapest and Singapore.

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.

Learn more at seon.io