Fraud & Risk in the Global Payments Era

SEON

A vertical excerpt of the 2025 Digital Fraud Outlook

Table of Contents

Introduction	3
Key Industry Trends Shaping Payments Fraud Prevention	5
How Payments Differs From Other Sectors	6
High-Risk Frontiers: Emerging Fraud Threats & Impact	7
AI: From Hype to High-Value in Payments	8
Underinvestment vs. Escalation — A Sector at Risk	9
The Payments Fraud Narrative: What the Data Tells Us	10
What Payments Providers Must Do Next	11
Top 3 Takeaways for Payments Fraud Prevention	12
Securing Trust at Transaction Speed	13
Want the Bigger Picture?	14
About SEON	15

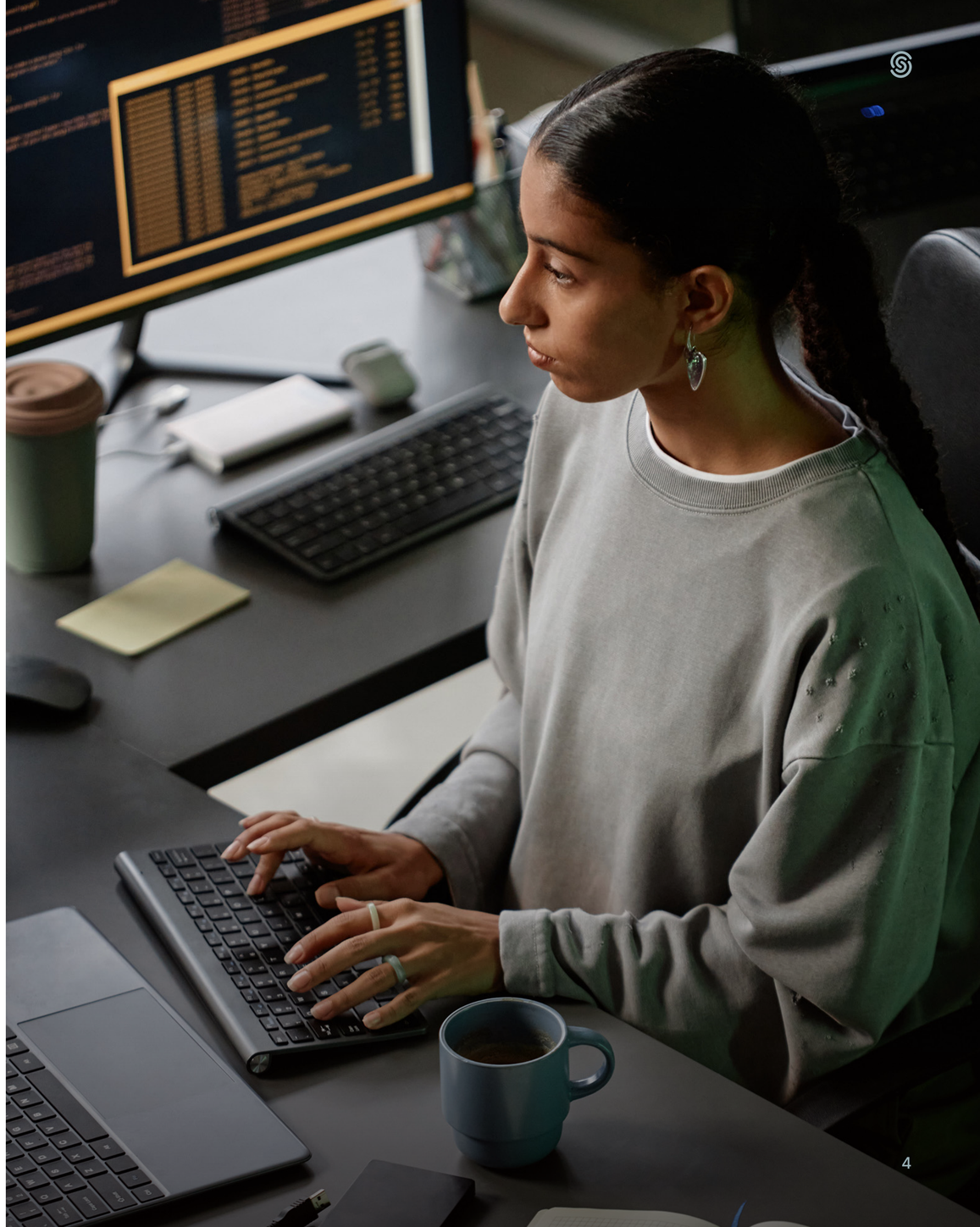
Introduction

Payments fraud in 2025 is defined by speed, sophistication and scope with an attack surface expanding as fast as innovation. Instant settlement has removed the safety nets of the past, giving fraudsters a decisive advantage if detection lags by even a second. Digital wallets and cryptocurrency, once niche payment methods, are now mainstream — and prime targets. Their appeal to customers mirrors their appeal to criminals: fast, frictionless and irreversible. Synthetic identities slip through onboarding, building credibility before draining accounts. Mule networks move stolen funds across borders in coordinated waves. Friendly fraud, in the form of chargeback abuse, quietly erodes margins, particularly for cross-border processors where dispute rates run markedly higher. Instant transfers add another layer of vulnerability, leaving no recovery window once a transaction is approved. Fraud risk across the sector drains revenue and can destabilize trust among providers, merchants and end users.

But fraud teams are fighting back. Real-time transaction monitoring is now the clear frontline defense, and AI-driven decisioning is gaining traction as providers seek ways to detect anomalies faster without choking customer experience. There's also a growing recognition that fraud and AML can no longer be treated as separate battles — the same mule account flagged for fraud today may trigger a compliance investigation tomorrow, and when viewed together these efforts can be streamlined into a single, more efficient defense.

Our latest research — drawn from 335 senior fraud, risk and compliance professionals across payments, financial services and fintech companies — reveals that while 85% of payments companies are increasing fraud prevention budgets, many remain constrained by legacy tooling and siloed data. This leads to high operational drag, missed threats and costly customer friction — exactly what fraudsters want to exploit.

But the market is racing to close that gap, moving from reactive detection to preemptive, real-time decisioning that can keep pace with money in motion today. In short, the payments industry is at a tipping point. The winners will be those who can predict and prevent threats upstream, uniting intelligence across silos and acting as quickly as the money moves.



Key Industry Trends

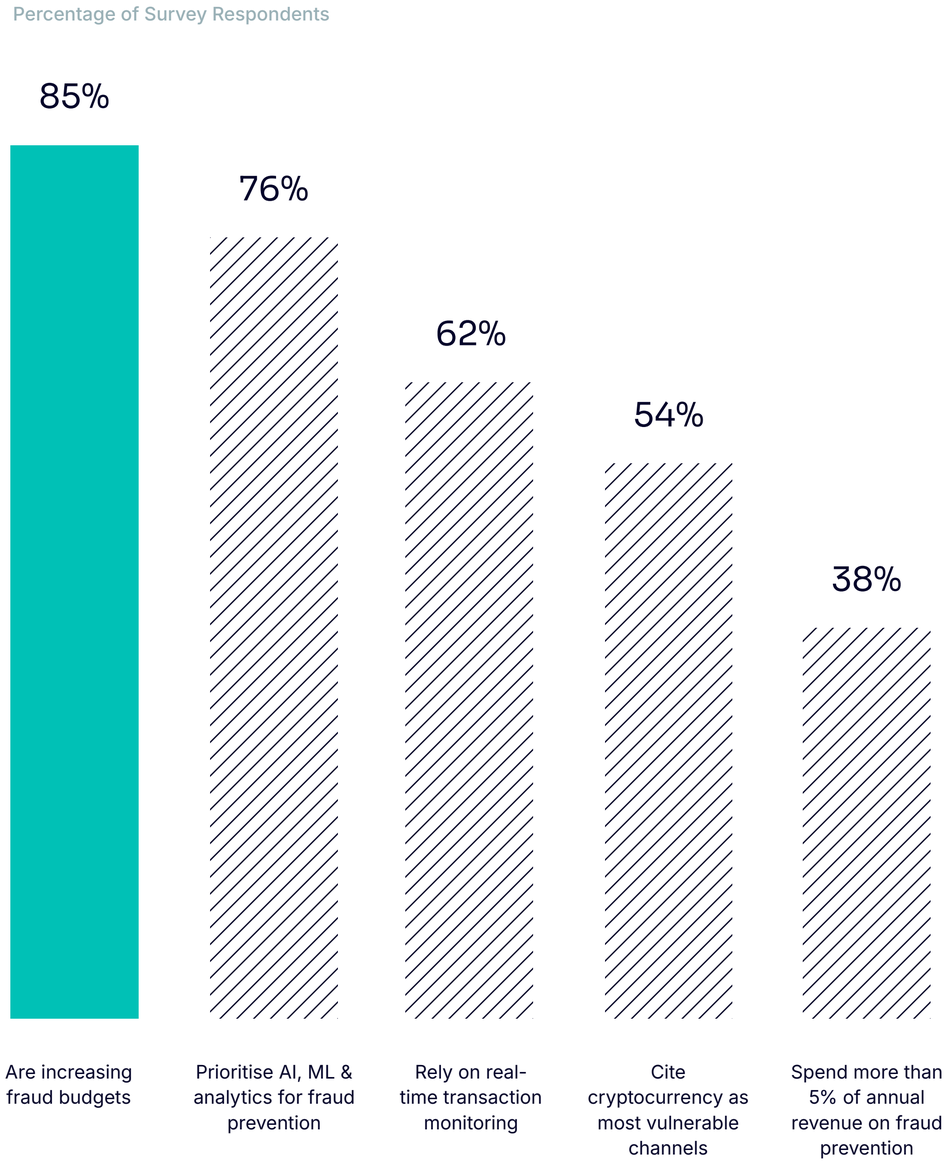
→ **Real-time transaction monitoring is now mission critical**
62% of payments organizations identify real-time transaction monitoring as their single most effective defense, driven by the speed and irreversibility of instant settlement rails.

→ **AI and advanced analytics are top capability priorities**
76% of surveyed organizations prioritize AI, machine learning and advanced analytics skills for fraud prevention — with 38% of payments firms emphasizing broad AI/ML expertise to enhance detection accuracy.

→ **Budgets are increasing — but ROI remains under scrutiny**
85% of payments companies are increasing fraud budgets, with 38% already spending more than 5% of their annual revenue on prevention, but without the right tools and integration, spending risks outpacing returns.

→ **Synthetic identity fraud is the fastest-growing threat**
Identity fraud losses are projected to hit $23 billion by 2030, with synthetic IDs leading the charge — exploiting onboarding processes that lack early, sophisticated prescreening.

→ **Digital wallets and crypto remain top attack surfaces**
54% of payment professionals cite cryptocurrency, and 38% cite digital wallets as their most vulnerable channels, noting the irreversible, high-speed nature of these transactions.



How ePayments Differs From Other Sectors

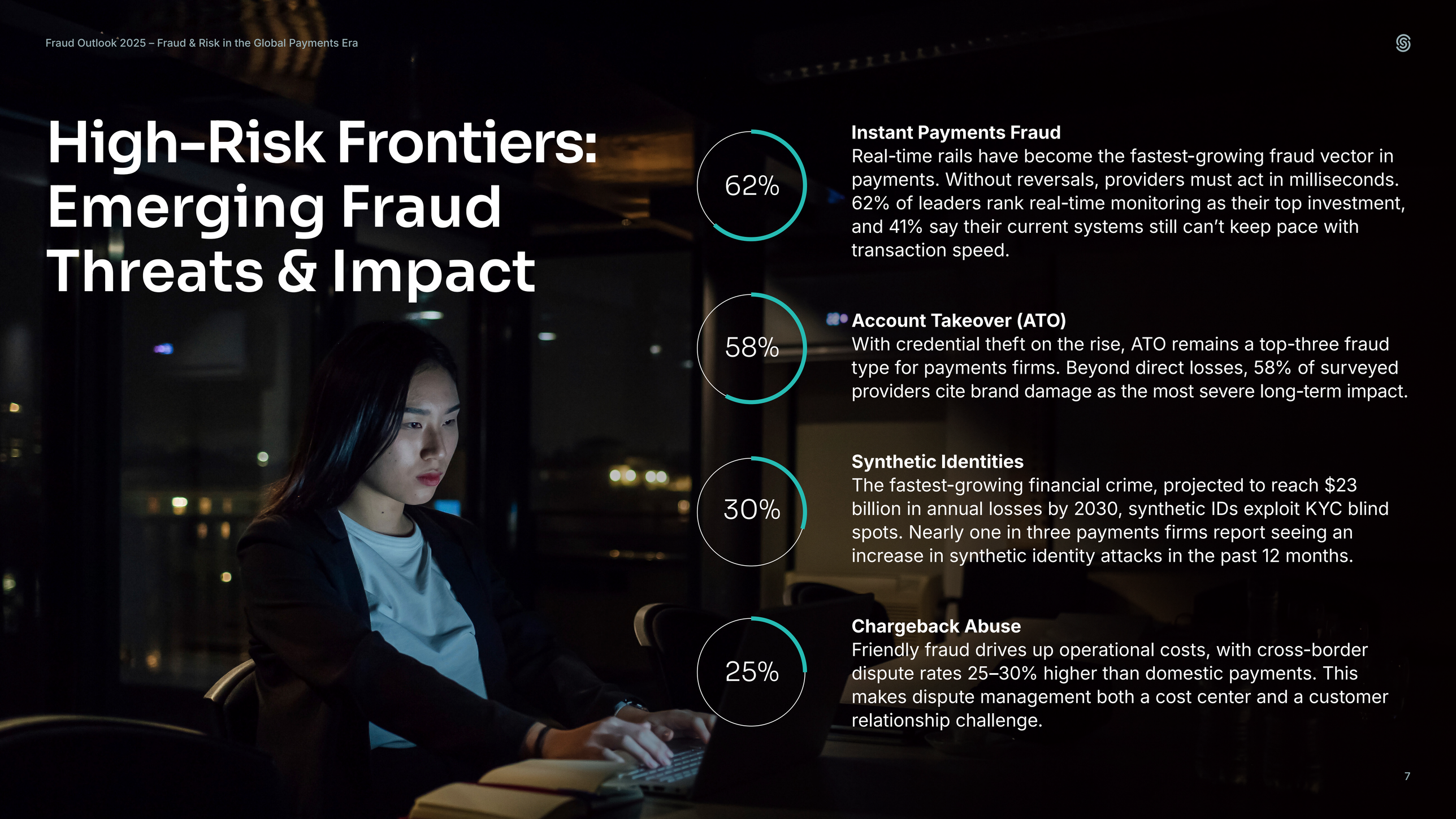
→ **Irreversibility & Velocity**
In card payments, chargebacks provide some recourse; in instant payments, the money is gone in seconds. There's no settlement window, no retrieval buffer — prevention is the only line of defense. This reality explains why 62% of payment leaders now prioritize upstream screening to stop fraud before transactions are initiated or approved.

→ **Counterparty Risk Exposure**
Every payment has at least two points of vulnerability: the sender and the receiver. Fraud can originate from either side (or both) through mule accounts, collusive merchants or compromised payees. Effective protection requires two-sided screening, mapping relationships and flagging risky counterparties in real time.

→ **High Regulatory Burden**
Payments firms must balance fraud prevention with compliance obligations, such as sanctions screening, politically exposed person (PEP) checks and anti-money laundering (AML) rules. A majority of respondents (64%) say that managing both fraud and AML initiatives within the same operational team would significantly improve efficiency, pointing toward unified platform use, especially in cross-border corridors.

→ **Customer Experience Sensitivity**
In any high-volume, low-margin sector, the user experience is as critical as fraud prevention. A single false positive or unnecessary delay can drive customers to competitors. 25% of payments leaders rank improved customer experience as the single most valuable outcome of fraud prevention, underscoring the need for dynamic friction that only intervenes when risk is real.

High-Risk Frontiers: Emerging Fraud Threats & Impact



62%

Instant Payments Fraud
Real-time rails have become the fastest-growing fraud vector in payments. Without reversals, providers must act in milliseconds. 62% of leaders rank real-time monitoring as their top investment, and 41% say their current systems still can’t keep pace with transaction speed.

58%

Account Takeover (ATO)
With credential theft on the rise, ATO remains a top-three fraud type for payments firms. Beyond direct losses, 58% of surveyed providers cite brand damage as the most severe long-term impact.

30%

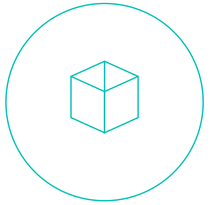
Synthetic Identities
The fastest-growing financial crime, projected to reach $23 billion in annual losses by 2030, synthetic IDs exploit KYC blind spots. Nearly one in three payments firms report seeing an increase in synthetic identity attacks in the past 12 months.

25%

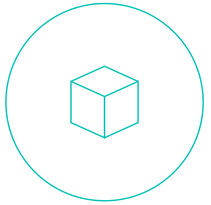
Chargeback Abuse
Friendly fraud drives up operational costs, with cross-border dispute rates 25–30% higher than domestic payments. This makes dispute management both a cost center and a customer relationship challenge.

AI: From Hype to High-Value in Payments

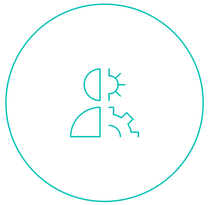
Artificial intelligence (AI) has moved from experimental to essential, but only when deployed with clarity and control.



AI Suggested Rules offer transparent decisioning, mapping each risk signal to a score and rationale. This is vital for audit-readiness and compliance defense.



AI Insights Score excels at uncovering hidden fraud patterns but risks over-blocking without oversight or transparency.



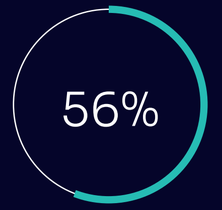
Hybrid Decisioning combines the strengths of AI and business rules, and is now the most adopted approach in high-risk payment flows.

76% of payments organizations are prioritizing AI, ML and analytics capabilities, **but only 51% say their current AI tools deliver measurable ROI.** The gap is often due to limited data integration and lack of explainability — both of which are solvable with modern, modular fraud tech.

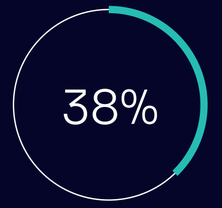
Underinvestment vs. Escalation — A Sector at Risk

The payments sector is spending more than ever, but fraud loss curves aren’t flattening.

of payments companies are increasing fraud budgets.



believe fraud losses are still outpacing revenue growth, signaling resource allocation and tooling gaps.



already spend over 5% of annual revenue on prevention.

Without modernizing core detection infrastructure, breaking down siloed data and integrating fraud and AML into a collaborative operational view, budget increases risk becoming just another overhead line, and not a source of competitive advantage.

The Payments Fraud Narrative: What the Data Tells Us

The payments ecosystem is balancing on a knife edge — driving record volumes while fending off more sophisticated, faster-moving attacks than ever before. The very factors fueling growth — speed, global reach and low friction — are the same that fraudsters exploit with precision.

The lines between fraud and financial crime are blurring. A mule account flagged for fraudulent transactions today could be the same entity routing illicit funds tomorrow. This overlap is why **more than six in ten payments leaders now see convergence between fraud prevention and AML as essential to their future operating model.**

The data confirms the challenge: fraud patterns are evolving across multiple fronts at once. This demands a shift in mindset, from chasing fraud after it happens to engineering systems that anticipate and neutralize threats before they surface. Those who unify intelligence across risk domains, shorten investigation cycles and inject automation where human teams are slow or burdened will be best positioned to stay ahead.

What Payments Providers Must Do Next:

Shift Prevention Further Upstream

Intercept risk before it reaches settlement or compliance workflows. Leveraging early-stage device fingerprinting, email/phone risk analysis and behavioral biometrics can cut fraud case volumes before it hits manual review queues, reducing both losses and operational strain.

Break Down the Fraud–AML Divide

Unify investigative tooling so analysts see the full picture in one view. This approach can trim average investigation times while revealing linked entities that would otherwise be missed in siloed systems.

Embrace Explainable AI at Scale

Providers adopting hybrid models that blend machine learning with rule transparency are reporting faster approval cycles and fewer false positives compared to AI-only or rule-only systems. The sweet spot is automation without losing the ability to justify a decision to regulators or partners.

Build Counterparty Intelligence

Map payment flows across both senders and receivers to spot mules and collusive merchants before funds move. Cross-border providers using this approach report sharper fraud detection without added friction for trusted counterparties.

Top 3 Takeaways for Payments Fraud Prevention

1. **Speed is Survival:** Real-time payments demand real-time defense. In instant payments, the detection window closes almost as soon as the transaction is initiated. Prevention, not post-event remediation, defines success.

2. **Unify Intelligence:** Siloed fraud and AML systems slow investigations. Treat fraud and AML as two halves of the same defense strategy to expose hidden threats and streamline operations.

3. **Value Beyond Loss Reduction:** Fraud prevention is a growth enabler: reducing churn, maintaining merchant trust and preserving competitive advantage in a sector where switching costs are low.

Securing Trust at Transaction Speed

The payments industry is entering a defining decade. The next wave of winners won't be those who simply spend more on fraud prevention — they'll be the providers who transform that investment into faster, smarter and more connected decision-making.

The sector's leaders are already shifting from detection to prediction. They're uniting fraud and AML operations to see the full risk picture, deploying AI models that learn and adapt without becoming a black box and embedding risk intelligence into every stage of the payment journey. These moves don't just cut losses; they strengthen trust at the exact moment it's earned — when the customer completes a transaction without friction or fear.

Fraudsters will keep innovating, but so will the defenses. In an environment where money moves in milliseconds and reputations can turn in minutes, the ability to stop threats before they materialize will define market leadership. The leaders of the next decade are already moving. The question is: will you meet fraud at its speed or let it set the pace?

Want the Bigger Picture?

This Payments report is just one slice of the 2025 Digital Fraud Outlook — SEON's most comprehensive analysis to date of the fraud, risk, and compliance landscape. Drawing on insights from 754 senior leaders across payments, financial services, fintech, eCommerce and iGaming, the report reveals how different industries are adapting to an era of faster money, smarter fraud tactics and mounting regulatory pressure.

Download the full report to:

→ **Benchmark** your fraud strategy against other sectors and geographies

→ **Explore** cross-industry innovations with proven results

→ **Identify** new approaches for turning fraud prevention into a revenue driver

Whether you operate in payments or across multiple verticals, the full outlook will give you a broader view of the trends, threats and technologies reshaping fraud prevention in 2025 and beyond.

SEON

About SEON

SEON is the command center for fraud prevention and AML compliance, helping thousands of companies worldwide stop fraud, reduce risk and protect revenue. Powered by 900+ real-time, first-party data signals, SEON enriches customer profiles, flags suspicious behavior and streamlines compliance workflows. With integrated fraud and AML capabilities, SEON operates globally from Austin, London, Budapest and Singapore. Learn more at seon.io.

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