COMPASS PLUS TECHNOLOGIES

From rules to intelligence:

How FIs can harness hybrid systems to stay ahead of evolving fraud

Introduction

If there's one constant in payments, it's fraud. It is a continuously evolving space, and as fraud systems become more sophisticated, so too do the fraudsters looking to exploit weaknesses. Juniper Research estimates that banks and payment providers could collectively face costs of $58.3 billion by 2030, up from $23 billion in 2025 — a stark reminder of the scale of the challenge ahead.

The increase isn't just about volume; it's about complexity. The way people bank and pay today is fundamentally different from even a decade ago. Consumers are using more payment methods, devices, and channels than ever before, giving fraudsters more opportunities to find vulnerabilities. On top of this, criminals are increasingly leveraging machine learning and other advanced tools to sharpen their tactics, creating a landscape where financial institutions must protect not only their customers, but also their revenue and reputation all in real time.

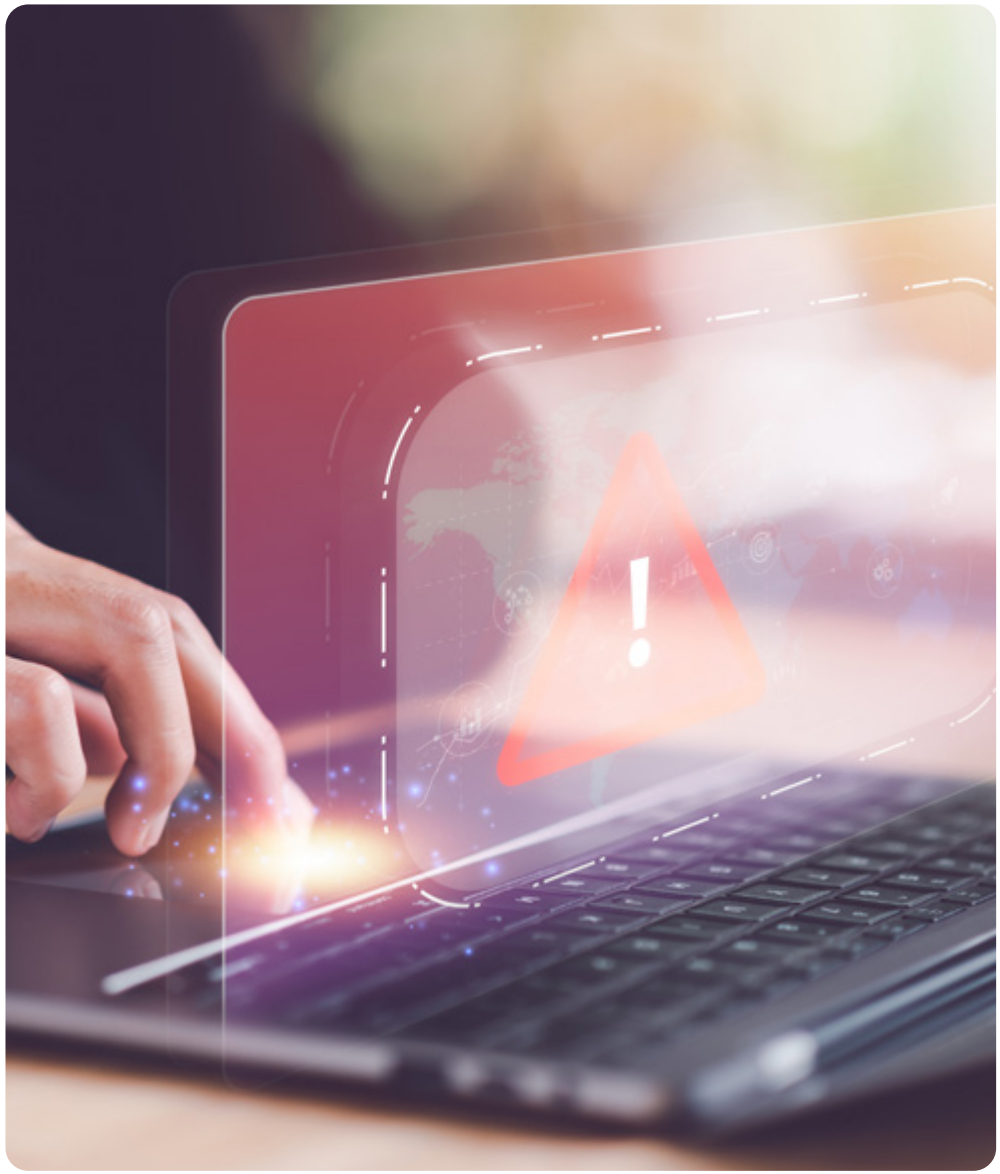
Key challenges for FIs

Despite banks spending more than $12.6 billion on anti-fraud tools*, many still feel like they are fighting a losing battle in the war against fraud. As such, FIs are constantly searching for the strategic edge that will allow them to:

- Respond quickly to new and evolving fraud schemes
- Increase detection accuracy while reducing false positives
- Identify fraud earlier and improve predictability
- Protect digital channels from emerging vulnerabilities
- Deploy adaptive fraud defence that scales dynamically without compromising performance

Yet, many financial institutions continue to rely on traditional rule-based systems to safeguard themselves and their customers — systems that, while effective for known patterns, struggle to keep pace with the speed and sophistication of today's fraud landscape.

**Coinlaw*



Traditional rule-based systems

Rule-based fraud detection has long been the industry's go-to for protecting transactions. Built on a series of predefined "if–then" conditions, these systems analyse real-time data across multiple sources — from location and transaction value, to frequency and device type — and act when something looks suspicious. The result might be a blocked transaction, a flagged alert, or a manual review.

While this approach has its strengths — such as speed, transparency, and proven reliability in tackling known fraud patterns — the reality is that fraud today evolves far faster than static rules can keep up with. Relying solely on rules creates significant operational overhead, disrupts the customer journey, and ultimately limits effectiveness.

Limitations of rule-based systems:

- **Limited flexibility:** Rule-based systems often operate with a set and forget mindset. Built on rigid "if X, then Y" logic, they struggle to capture the complexity of real-world behaviours or adapt to emerging fraud tactics as rules won't update to reflect these changes unless they're being updated. Instead, they demand frequent manual updates and reviews — a growing challenge as alert volumes rise 30–40% each year*, creating bottlenecks and slowing down responses to real threats (*Trust Decision)
- **Higher false positives:** Rules lack nuance. Genuine transactions are too often flagged as fraudulent, generating creating unnecessary investigations, customer friction, and additional operational costs. In fact, around 15% of transactions are sent for manual review, yet 72% of those alerts prove to be false alarms**, creating unnecessary friction and wasted effort (**ACAMS)
- **Limited scalability:** As transaction volumes and complexity grow, static rules simply can't keep pace. Each new rule must be manually coded and tested, making scale slow, resource-heavy, and prone to error. This lack of adaptability makes it harder for financial institutions to stay ahead of increasingly sophisticated fraud schemes

The reality is that fraud is no longer static, and financial institutions cannot afford to rely on tools that are. While rule-based systems still have their place, if rules are applied alone their set and forget mindset, high false positive rates, and lack of scalability make them ill-suited to today's dynamic threat landscape.

Financial institutions need solutions that combine the clarity of rules with the adaptability of advanced analytics and machine learning — balancing protection, operational efficiency, and customer experience.

Machine learning

Machine learning is fast becoming the cornerstone of modern fraud detection, thanks to its ability to continuously learn, adapt, and uncover new patterns of criminal activity as they emerge.

Unlike traditional rule-based systems, machine learning analyses vast volumes of data in real time, learning from historical patterns while dynamically adapting to new threats. It identifies subtle correlations, anomalies, and behaviours that static rules would miss, spotting fraud that might otherwise go undetected.

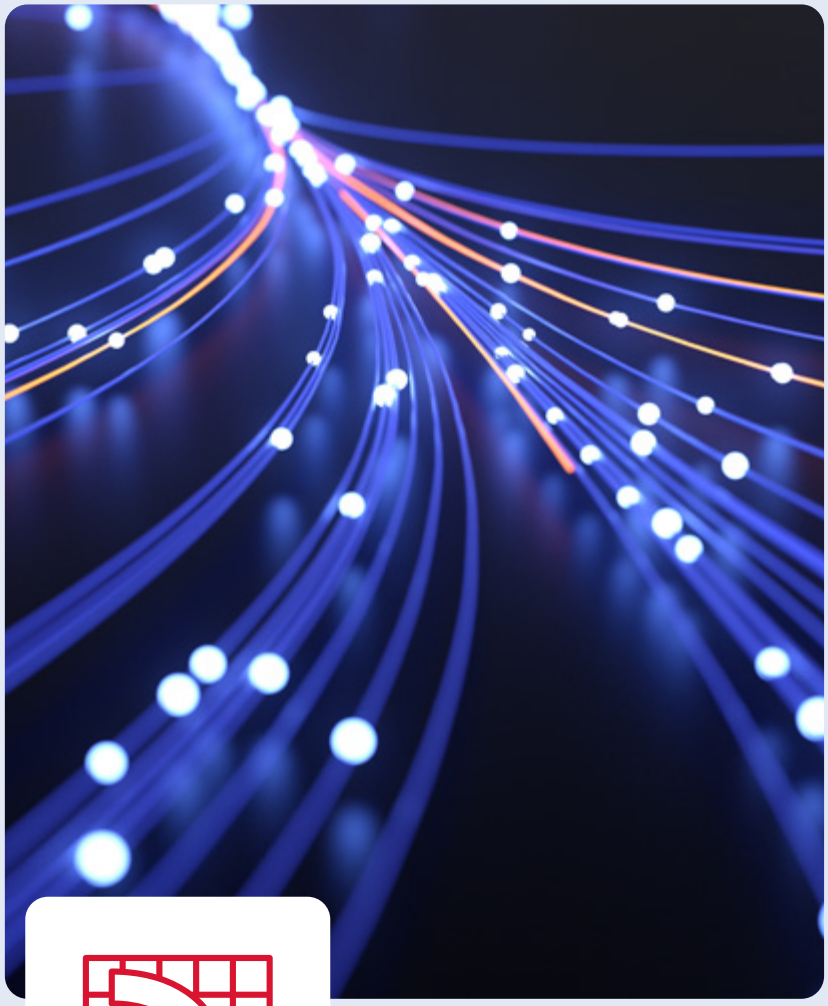
For financial institutions, the benefits are clear: machine learning reduces false positives by adding context and nuance to decision-making, meaning fewer genuine transactions are declined and more investigative effort is focused on high-risk cases. As the technology learns and evolves, it not only strengthens protection but also enhances the customer experience, delivering faster, frictionless transactions without compromising security.

Why machine learning?

- **Self-adaptive learning:** Machine learning doesn't stand still. It evolves with every new data point, automatically refining models to recognise emerging fraud tactics that static rules would miss
- **Greater accuracy, fewer false positives:** By understanding real patterns in the data and dynamically adapting to them, machine learning improves detection rates while keeping genuine transactions flowing — reducing false alarms and customer frustration
- **Efficiency at scale:** By reducing manual intervention and false positives, fraud teams can focus on high-risk cases, improving operational efficiency and lowering costs
- **Profile stability:** By building a deep understanding of customer behaviour and transaction history, machine learning spots irregularities — from sudden changes in spending to unusual withdrawal patterns — before they escalate into fraud
- **Anomaly detection:** Acting as a disruption detector, machine learning can be trained to highlight unexpected behaviour in transactional data. Trained on historical transaction patterns, it can quickly separate the regular from the anomalous, alerting teams to potential fraud in real time

Together, these capabilities show why machine learning is no longer optional for modern fraud prevention — it's essential. By continuously learning, spotting anomalies, and understanding customer behaviour, machine learning not only strengthens detection but also reduces operational burden and protects the customer experience.

For banks and financial institutions, the message is clear: staying ahead of fraud today means adopting solutions that evolve as fast as the threats they're designed to stop.



AI can lower false alarms by 45%

McKinsey

Hybrid approach

While machine learning brings speed, adaptability, and intelligence to fraud detection, it doesn't need to replace rule-based systems entirely. In fact, the most effective approach often lies in blending the two: leveraging the clarity and transparency of rules with the predictive power of machine learning. This hybrid model enables FIs to tackle both known and emerging threats, balancing operational efficiency with robust protection — and ultimately delivering a safer, smoother experience for customers.

By combining rule-based frameworks with machine learning, FIs can implement dynamic, real-time risk scoring that addresses a wide spectrum of fraud patterns. This approach preserves the clarity and accountability of rules while harnessing machine learning's ability to detect subtle, sophisticated schemes that static systems would miss.

The impact goes beyond detection. McKinsey reports that AI can lower false alarms by 45%, significantly reducing alert volumes, easing the burden on fraud teams, and reducing costs. For financial institutions, this translates into faster, more accurate decisions, fewer operational bottlenecks, and a more seamless experience for customers. As fraud tactics continue to evolve, hybrid systems are no longer just an innovation — they're an essential strategy for staying ahead of increasingly sophisticated threats.

Key takeaways

Machine learning is no longer optional:

In 2025, fraud is being fought on a digital battleground. Criminals are using advanced tools, and financial institutions must match that speed and sophistication to stay protected

Hybrid approaches deliver results:

Combining rule-based systems with machine learning delivers both clarity and adaptability, helping FIs detect known threats while staying ahead of emerging fraud patterns

Efficiency and accuracy go hand in hand:

Machine learning reduces false positives and alert volumes, freeing fraud teams to focus on genuine threats and improving the customer experience

Fraud prevention must evolve:

In the age of AI-powered fraud, adopting intelligent, adaptive solutions is no longer a luxury — it's a necessity for staying secure, agile, and competitive

COMPASS PLUS
TECHNOLOGIES

Compass Plus Technologies

enquiries@compassplustechnologies.com

compassplustechnologies.com

Copyright © 2025 Compass Plus (Great Britain) Limited. All rights reserved.