Next Level Compliance:

AI in Payments Transaction Monitoring and Financial Crime Prevention

Part 2

The regulatory implications for AI-based transaction monitoring

Part 2

The regulatory implications for AI-based transaction monitoring

The Instant Payments Regulation and the EU AI Act set the framework for the use of AI in transaction monitoring, reshaping the operational processes in payments and compliance.[1] The second part of our three-part series Next Level Compliance: AI in Payments Transaction Monitoring and Financial Crime Prevention clarifies what 'real time' means and how to build explainable AI across AML, fraud and sanctions. We also look at the operating model, governance and latency choices needed to stay compliant without adding friction.

Instant Payments Regulation

Within the framework of the Instant Payments Regulation (Regulation (EU) No. 2024/886), a move away from transaction-based to customer-based monitoring was introduced, with negative impact on the possibilities of using AI in real-time transaction monitoring. This is because it lacks the transaction data from which AI systems can learn. Thus, a valuable possibility for network analysis is missing, so the fight against money laundering and the possibility of reducing false positives in particular are made more difficult. However, it is, of course, still possible to monitor transactions in real time. Two scenarios are possible to still be able to use the advantages of AI:

- Transactions are monitored in real time, but without interfering with transaction processing. The findings are used to improve the accuracy of customer-related matching and as an additional source for downstream analysis of payment transactions.

- Transactions are monitored in real time and continue to have an immediate impact on transaction processing, but not on sanction lists. This, of course, creates powerful systems to prevent the high rejection rates feared by the regulator. Customer-related monitoring is also carried out as specified by the regulator.

Integration of AI tools in compliance processes

While the regulation encourages innovation, many institutions face challenges in operationalizing AI within existing transaction monitoring and Know Your Customer (KYC) systems. AI can significantly enhance anomaly detection and identity verification, but achieving regulatory trust, explainability and data quality remains complex.

Positive outcomes and synergy potential

Enhanced KYC processes through AI integration. The intersection between instant payments and KYC offers opportunities to leverage AI and machine learning for faster, more accurate identity verification and risk scoring. Data generated through instant transactions can feed into dynamic customer profiles and continuous monitoring.

Verification of Payee and list matching synergies. The Verification of Payee (VoP) requirement aligns with existing list-matching processes (e.g. sanctions, PEP, or adverse media screening). Although the evaluation logic differs, shared infrastructure and AI-assisted matching can create operational efficiencies and reduce false positives.

Improved customer trust and market competitiveness. The transparency and speed of instant payments are expected to enhance customer trust and enable new digital business models (e.g. on-demand services, real-time treasury management and embedded finance).

Example of a transaction monitoring enhancement

Capco's long-standing partner Hawk's AI AML Overlay enhances transaction monitoring by incorporating a customer's existing data into its analysis. This existing data includes information such as historical transactions, behavior patterns, and risk profiles.

Rather than relying solely on real-time transaction data, Hawk uses advanced AI techniques to detect anomalies based on the full context of customer behavior. This approach allows for more accurate and explainable detection of suspicious activity, even in a customer-based monitoring framework, while seamlessly integrating with existing systems to make the most of available data.

EU AI Act: practical implications for payments

Most risk-related AI in payments will be treated as high risk under the EU AI Act or by prudential supervisors adopting the Act's principles. Firms should therefore plan to comply with the full set of obligations: a documented risk management system, robust data governance and quality controls, technical documentation sufficient for audit and supervisory review, event logging and traceability, clear user information and operating instructions, human oversight with defined authority and escalation, targets for accuracy, robustness, cybersecurity and post market monitoring with incident reporting.

Explainability beyond transparency

In practice, explainability is essential to make these obligations effective and to satisfy internal audit and regulators. Important factors are:

- **Design time.** Maintain model cards and data set 'datasheets', link features to policy rationale, record assumptions and limitations, and 'harden' models with sensitivity and stability testing before go live.

- **Decision time.** Generate a concise, human readable rationale for each alert or decision (e.g. top contributing features, reason codes, and, where appropriate, counterfactuals). Surface these within case management so investigators can act without digging through notebooks.

- **Lifecycle.** Monitor drift, performance and fairness across customer segments, run challenger models, and keep immutable logs for reproducibility and disclosure.

Operating impacts for payments

Latency budgets in instant payments require explainability that does not slow down the flow. Use pre computed feature attributions for common patterns, cache reason code templates, and provide deeper drill downs asynchronously to investigators. Establish cadence for a model risk governance (approval, periodic review, material change assessment) with clear ownership across first and second lines. Align data minimization and privacy constraints with monitoring needs via feature stores, pseudonymization and defensible retention schedules.

Real-time monitoring defined

In fraud prevention, 'real time' means the system evaluates payment during processing and can block or step up before completion, typically within tens to hundreds of milliseconds. By contrast, 'near real time' AML processing can occur seconds or minutes after the event and is suitable for post facto flagging rather than interdiction. Precision at speed matters: overstating real-time capability creates control gaps and delivery risk. Banks should design end to end flows - risk scoring, orchestration and customer treatment - that meet latency budgets while minimizing friction.

Conclusion: human oversight for accountability and improved customer experience

The Instant Payments Regulation is both a technological and regulatory catalyst for the European payments ecosystem. While it imposes significant operational and compliance challenges, it also provides banks and PSPs with opportunities to modernize their infrastructure, enhance customer experience and leverage AI to transform compliance and transaction monitoring processes.

At the same time, under the EU AI Act, high risk AI demands clearly defined roles for performance monitoring, adjudication of 'edge cases' and remediation of adverse outcomes. Human-in-the-loop review for material decisions remains essential. Transparent communications and timely recourse will enhance customer trust, but additional controls must not erode the speed advantages of instant payments.

How Capco can help

Capco enables banks, payment providers and fintechs to deploy AI-enabled monitoring that meets regulatory expectations and delivers measurable impact. We run rapid diagnostics and design target operating models, modernize data and orchestration, accelerating time-to-value through our regulatory and operational expertise and experience. Contact us to find out more.

References

1. https://eur-lex.europa.eu/eli/reg/2024/886/oj/eng and https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng

Authors

Wesselin Kruschev
Managing Principal

Contact

Jan Stüve
Partner
Jan.Stueve@capco.com

About Capco

Capco, a Wipro company, is a global management and technology consultancy redefining transformation across the financial services and energy industries. Capco leverages the power of AI and our deep domain expertise to help our clients move faster, make smarter decisions, and drive greater impact. Our award-winning Be Yourself at Work culture and diverse talent drive bold, forward-thinking ideas and lasting change.

To learn more, visit **www.capco.com** or follow us on LinkedIn, Instagram, Facebook, and YouTube.

Worldwide Offices

APAC	EUROPE	NORTH AMERICA
Bengaluru – Electronic City	Berlin	Charlotte
Bengaluru – Sarjapur Road	Bratislava	Chicago
Bangkok	Brussels	Dallas
Chennai	Dusseldorf	Houston
Gurugram	Edinburgh	New York
Hong Kong	Frankfurt	Orlando
Hyderabad	Geneva	Toronto
Kuala Lumpur	Glasgow	
Mumbai	London	**SOUTH AMERICA**
Pune	Milan	Rio de Janeiro
Singapore	Paris	São Paulo
	Vienna	
MIDDLE EAST	Warsaw	
Dubai	Zurich	

capco.com

CAPCO
a **wipro** company