CAPCO

Next Level Compliance:

AI in Payments Transaction Monitoring and Financial Crime Prevention

Part 1

How AI is transforming payments and financial crime monitoring

Part 1

How AI is transforming payments and financial crime monitoring

Payments are moving to real time, regulations are tightening and fraud typologies are evolving faster than rulesets. Traditional, siloed, rule-based transaction monitoring leads to high false positives, costly manual reviews and blind spots for emerging threats. A modern, AI-enabled and integrated approach across fraud, AML and sanctions is essential to deliver faster, more accurate decisions while maintaining regulatory compliance.

In our three-part series, Next Level Compliance: AI in Payments Transaction Monitoring and Financial Crime Prevention, we will examine the following topics:

Part 1: What is wrong with today's transaction monitoring and how AI is transforming Anti-Money Laundering (AML), fraud prevention and sanctions and embargo screening.

Part 2: The regulatory implications for AI-based transaction monitoring.

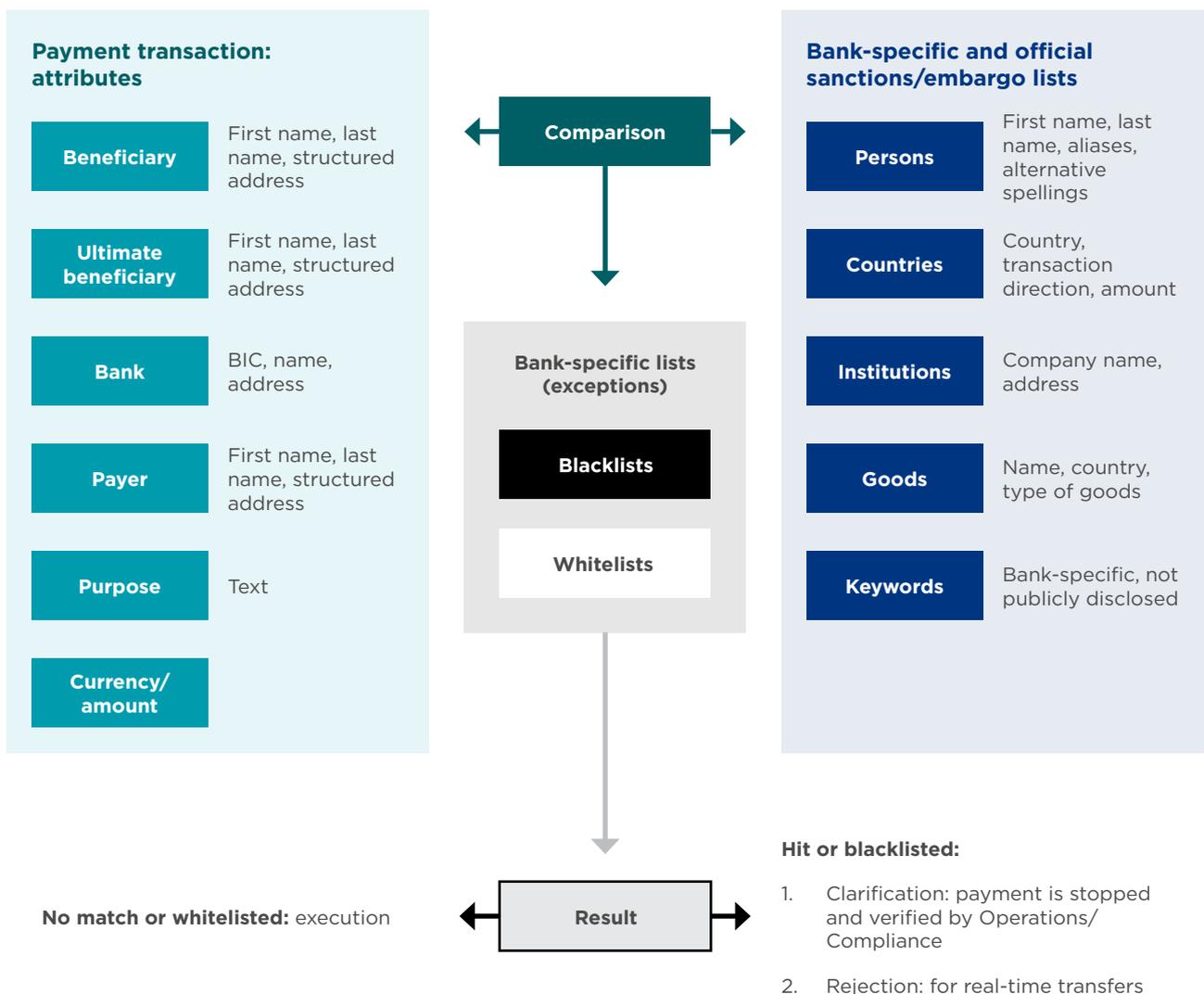**Part 3:** AI-driven business opportunities in financial crime prevention.

In this series, examples are drawn from Capco's long-standing partner Hawk's innovative platform to illustrate how artificial intelligence is redefining transaction monitoring and enabling financial institutions to stay ahead of emerging risks.[1]

Today's transaction monitoring

Most institutions still run separate stacks and teams for fraud, AML and sanctions. Fraud and sanctions screening typically happen pre-transaction while AML often triggers post-event and reports to authorities (e.g. the Financial Intelligence Unit in Germany). Tools remain predominantly rule-based: banks must pre-define scenarios, which leads to poor detection of emerging patterns and a constant trade-off between missing risk (false negatives) and overwhelming operations teams (false positives). As volumes grow, manual hit resolution becomes a cost and latency bottleneck, especially where timely approval or rejection is required. Legacy platforms also struggle with today's data richness and quality demands. Even with standardization improvements (e.g. structured addresses), older systems often cannot scale or adapt to new payment rails and regulatory expectations, forcing institutions to consider modernization.

Schematic view of a transaction monitoring process

Payment transaction: attributes

Beneficiary	First name, last name, structured address
Ultimate beneficiary	First name, last name, structured address
Bank	BIC, name, address
Payer	First name, last name, structured address
Purpose	Text
Currency/ amount	

Comparison

Bank-specific lists (exceptions)

Blacklists

Whitelists

Bank-specific and official sanctions/embargo lists

Persons	First name, last name, aliases, alternative spellings
Countries	Country, transaction direction, amount
Institutions	Company name, address
Goods	Name, country, type of goods
Keywords	Bank-specific, not publicly disclosed

Result

No match or whitelisted: execution

Hit or blacklisted:

1. Clarification: payment is stopped and verified by Operations/ Compliance

2. Rejection: for real-time transfers

Instant payments change the game

Instant payments (IP) eliminate the buffer for human intervention. Controls must operate inline, at millisecond latency, with high precision. Real-time rails have proven more attractive targets for social-engineering and account-takeover fraud attempts. Experience from existing IP markets shows attacks rates are several times higher compared to those in traditional SEPA batch processing. In short, instant payments can mean instant fraud unless controls become both faster and smarter.

Unifying fraud, AML and sanctions

Historically, separating fraud from compliance was acceptable when decisions could be made after settlement. In a real-time world, it is counterproductive. The same data, features, and analytic techniques — graph analysis, anomaly detection and behavioral profiling — benefit all three domains. An integrated operating model reduces duplicated effort, aligns decisions, and improves risk coverage at the point of payment.

Where AI adds value (and where it doesn't)

Data and features. Unified ingestion across payments, customer, device and external data, as well as entity resolution and risk-relevant feature engineering enable models to learn behaviors, not just thresholds.

Real-time detection. Machine-learning and graph models score transactions in-flight, detect anomalies and surface links across entities that static rules miss. Hybrid approaches retain business rules for hard constraints while letting models handle nuance and novelty.

Triage and case prioritization. AI reduces alert noise, ranks cases by expected risk and generates investigator copilots to summarize context, freeing analysts to focus on true risk.

Continuous learning. Feedback loops from investigator decisions and regulatory outcomes adapt models as typologies change.

Where AI is less effective. Statutory checks with fixed logic (e.g. some list-matching rules) and formal regulatory reporting formats remain best handled with deterministic controls as it is done currently.

Modernization without 'rip and replace'

Full platform swaps are disruptive. Many banks succeed with overlays that sit alongside and integrate seamlessly with existing monitoring and case-management systems, adding real-time scoring, alert optimization and analyst tooling while legacy capabilities continue in parallel.[2] Where deeper change is required, staged legacy modernization can de-risk the journey by decoupling data, externalizing rules and incrementally migrating use cases.

Governance, explainability and compliance-by-design

AI in compliance must be auditable. This means maintaining model governance (versioning, validation, drift monitoring), robust documentation and human-in-the-loop review for material decisions. Use explainability techniques to justify outcomes to internal audit and regulators. Align with regulatory expectations on data quality, fairness and traceability. Integrate controls such as pre-deployment testing, challenger models, performance SLAs and access controls.

Artificial intelligence in AML

Traditional AML monitoring relies on predefined scenarios that struggle with fast-evolving laundering techniques. AI augments these controls by learning behavioral patterns across customers, accounts and counterparties. Unsupervised anomaly detection spots deviations from typical behavior, while supervised models classify customer and transaction risk using historical outcomes. Graph-based network analysis surfaces hidden relationships and transaction chains that are indicative of layering and structuring. Institutions increasingly automate elements of suspicious activity reporting — from narrative drafting to data pre-population — improving consistency and shortening turnaround times.

Benefits of applying AI to AML (source: The Global Treasurer)[3]

| **70%**	**5%**	**80%**	**$14bn**
Reduction in false positive alerts	Increase in the number of detected suspicious transactions	Reduction in investigation time of suspicious transactions	Potential global savings in AML alert optimization

Fraud prevention

Fraud controls must operate in real time, especially on instant-payment rails. Behavioral analytics build profiles at the user, device and channel levels to detect anomalies such as unusual payees, amounts or login patterns. Real-time scoring classifies each transaction's likelihood of fraud and triggers dynamic step-ups or holds when risk exceeds tolerance. Predictive models leverage historical fraud outcomes and near-misses to anticipate emerging attack vectors, while feedback loops from investigators continuously refine thresholds and features to minimize customer friction.

Hawk's real-time fraud analytics
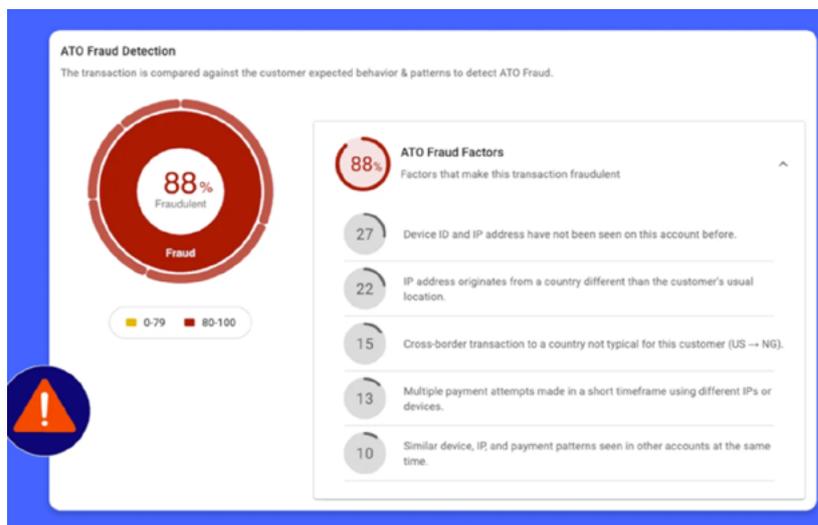
Sanctions and embargo screening

AI strengthens list screening by improving 'fuzzy' name matching and entity resolution — key for handling transliterations, nicknames, and incomplete data. Natural language processing models interpret context to reduce false positives from coincidental matches. Geospatial and routing checks add further confidence by assessing whether parties, banks or payment routes intersect with sanctioned regions. Deterministic rules remain necessary for statutory requirements, while AI can focus on ambiguous, suspicious cases.

Models and data required for effective monitoring

Effective AI in compliance depends on appropriate learning paradigms and high-quality data. Supervised learning supports risk scoring and prioritization; unsupervised techniques discover unknown typologies and anomalies; and reinforcement learning can optimize sequential decisions in real-time interventions. Representative examples include logistic regression and gradient-boosted trees for classification, autoencoders and isolation forests for anomaly detection and graph neural methods for relationship discovery. Training requires a unified data estate that combines transaction attributes, customer and counterparty profiles, device and channel signals, external watchlists and adjudication labels. Robust data governance — lineage, quality controls, and privacy safeguards — is essential to ensure valid outputs and regulatory acceptance.

Conclusion

To meet the speed and complexity of modern payments, institutions must converge fraud, AML and sanctions into a single, AI-enabled capability. Start by unifying data and features, introduce real-time hybrid scoring and modernize incrementally through overlays or staged replacement. The result is fewer false positives, better detection of emerging risks and compliance that keeps pace with instant payments.

A pragmatic approach blends deterministic controls with AI-driven analytics, governed by robust risk management models and clear documentation. Banks that unify these capabilities across AML, fraud and sanctions will achieve materially better detection at lower operational cost while preserving customer experience.

How Capco can help financial institutions establish a next-level compliance organization

At Capco, we help financial institutions unlock the full potential of artificial intelligence to transform their transaction monitoring capabilities. With deep industry expertise and a proven track record in regulatory compliance, data strategy and technology implementation, we partner with clients to design and deploy AI-driven solutions that deliver tangible results.

We combine domain knowledge with advanced analytics and modern architecture to help organizations move beyond traditional rule-based systems. Our consultants work closely with clients to reimagine transaction monitoring frameworks, optimizing alert efficiency, reducing false positives and enabling faster, more accurate detection of suspicious activity.

Through strategic partnerships with innovative technology providers such as Hawk, Capco delivers end-to-end support, from AI model selection and data integration to governance, testing and regulatory alignment. The result is a scalable, explainable and future-proof monitoring ecosystem that not only meets compliance requirements but also creates operational and competitive advantage.

Whether you are looking to enhance your systems, modernize legacy systems or build a next-generation AI-powered transaction monitoring platform, Capco can guide you through every step of the journey, helping you turn AI potential into real value.[4] Contact us to find out more.

References

1. Capco and Hawk have been long-standing partners, bringing together Capco's deep domain expertise in financial services with Hawk's cutting-edge AI-driven transaction monitoring technology. This collaboration enables our clients to enhance their financial crime prevention frameworks, leveraging advanced analytics, machine learning and real-time anomaly detection.

2. For example, HAWK's AML AI Overlay integrates seamlessly with existing transaction monitoring case systems, avoiding the need for a costly 'rip and replace' option when it comes to modernizing legacy systems.

3. https://www.theglobaltreasurer.com/

4. To find out more about Capco's Legacy Modernization Toolkit, watch a short video here.

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
Bengaluru – Electronic City
Bengaluru – Sarjapur Road
Bangkok
Chennai
Gurugram
Hong Kong
Hyderabad
Kuala Lumpur
Mumbai
Pune
Singapore

MIDDLE EAST
Dubai

EUROPE
Berlin
Bratislava
Brussels
Dusseldorf
Edinburgh
Frankfurt
Geneva
Glasgow
London
Milan
Paris
Vienna
Warsaw
Zurich

NORTH AMERICA
Charlotte
Chicago
Dallas
Houston
New York
Orlando
Toronto

SOUTH AMERICA
Rio de Janeiro
São Paulo

capco.com

in ⃝ f ▶

CAPCO
a **wipro** company

JN_7400