

The Transaction Monitoring Dilemma

# **Human Intuition or Machine Intelligence?**

## TABLE OF

# Contents

01	Introduction - The Case for Change	03
02	The Problem with the 'Either/Or' Mindset	04
03	Machine Intelligence – The Analytical Engine	05
04	The 'Human' Touch - The Context Engine	06
05	The Power of the 'And' – The Hybrid Solution	07
06	Solving the Dilemma	08
07	Implementing a Hybrid Model – Practical Steps	10
08	The Co-pilots of Transaction Monitoring	11
09	Sources	12
10	Flagright & FINTRAIL	13



The use of artificial intelligence (AI) to combat financial crime has gained momentum in recent years. Many regulated firms are integrating AI and Regulatory Technology (RegTech) into their anti-financial crime (AFC) control frameworks to enhance detection and support operational efficiency. In transaction monitoring (TM) specifically, AI and machine learning (ML) is shifting the industry away from static, rules-based systems toward real-time, behaviour-based approaches.

As criminal networks adapt their strategies and exploit technologies, the deployment of AI transaction monitoring models can help firms keep pace with the changing nature of financial crime. However, increasing reliance on AI raises important questions around the continued need for human insight and oversight.

This whitepaper explores why the future of transaction monitoring is not about replacing human investigators with machines, but about building smarter, more adaptive financial crime controls that combine the strengths of both. We explore how the shift from the "either/or" mindset to a hybrid model, merging AI's speed and scale with human judgement, offers the most effective path forward.

## The Case for Change




The long-standing challenges in transaction monitoring are well documented: high false positive rates, low conversion rates, and inefficient, manual processes that strain human resources. These limitations are compounded by increasing transaction volumes and complexity of financial products. Research by SWIFT<sup>1</sup> has indicated that typical transaction monitoring systems produce false-positive rates of around 70–95%, with the proportion of alerts converting to suspicious transaction or activity reports (STRs/SARs) often sitting as low as 2–10%.

In an AI-driven world, fears persist that automation could replace human roles, particularly in repetitive or rule-based functions. But when it comes to TM, the goal should not be replacement—it should be augmentation. AI offers unmatched speed and data-processing capacity, while humans provide contextual understanding, ethical reasoning, and critical oversight. Global standard-setters, including the FATF<sup>2</sup>, have called for a shift towards more dynamic, data-driven monitoring approaches underpinned by stronger explainability.

Clinging to a binary "human or machine" mindset risks keeping firms trapped in outdated, reactive models. Innovation lies in combining capabilities to build resilient, forward-looking systems aligned with evolving risks and expectations.

# The Problem with the 'Either/Or' Mindset

Relying solely on AI when it comes to transaction monitoring presents clear risks for firms:

- |   |  |
|---|--|
|  <b>Lack of contextual understanding</b> | Pattern recognition without understanding context can lead to both missed suspicious activity and an overwhelming volume of false positives. |
| <hr/>   |  |
|  <b>Model drift</b>                      | Without ongoing validation, AI models degrade over time as data patterns shift.  |
| <hr/>   |  |
|  <b>Model bias</b>                       | AI systems can learn and amplify biases present in training data, potentially leading to discriminatory outcomes.                            |

Firms that fail to monitor, recalibrate, and govern AI models risk undermining the very controls they aim to improve. Regulatory bodies such as the European Banking Authority (EBA)<sup>3</sup> have raised concerns about the uncritical adoption of RegTech solutions without proper testing, contextual calibration, or skilled oversight. These risks in particular stem from firms implementing solutions without testing their reliability or recalibrating parameters in line with the firm's business model, customers and risk exposure, alongside the concern that firms are struggling to understand AI technology and its capabilities.



On the other hand, relying exclusively on human investigators is increasingly unsustainable. The volume of transactions processed daily has outpaced the capacity of manual teams. Rules-based systems generate large volumes of low-value alerts, contributing to alert fatigue and increasing the risk of genuine threats being overlooked. Human-led systems alone cannot adapt quickly enough to changes in typologies, customer behaviour, or geopolitical factors. As financial products and customer behaviours grow more diverse, the complexity of transaction patterns makes it very difficult for even the most skilled analysts to detect suspicious activity or patterns without technological support.

To remain effective, TM systems must blend human and machine intelligence, capitalising on the strengths of both while mitigating their weaknesses.



# Machine 'Intelligence' - The Analytical Engine

Well trained AI transaction monitoring models can transform the way transaction monitoring is performed. Some of its benefits include:

## Speed



Real-time monitoring for immediate detection

## Scalability



Handles millions of transactions per second

## Pattern recognition



Identifies complex and hidden relationships

## Behavioural profiling



Learns customer norms and flags deviations

## Risk identification



When fed rich customer, device and behavioural context, it can drive risk-relevant outcomes

Global regulators are increasingly supportive of responsible AI adoption. In recent years we have seen bodies like the Financial Action Task Force (FATF) and the Financial Conduct Authority's (FCA) call for dynamic, data-driven monitoring systems to support the efforts in combatting financial crime.

The UK government promotes the safe and responsible use of AI in the UK financial market and encourages the market to leverage AI in a way that drives beneficial innovation. The FCA has also echoed this sentiment and outlines its approach<sup>4</sup> to AI following the Government's publication of its pro-innovation strategy on AI<sup>5</sup> and its AI regulatory principles guidance for Regulators<sup>6</sup>. This is further encouraged by the FCA's AI Live Testing programme which is a practical collaborative way for firms and the FCA to explore methods to assure the safe and compliant use of AI systems together. The FCA opened applications in July 2025, with testing slated to begin in autumn 2025 via the Supercharged Sandbox with NVIDIA. The FCA has also encouraged the responsible use of new technologies to meet AML/CFT obligations.



*"There are also many potential benefits for financial services firms including enhanced data and analytical insights, increased revenue generation, increased operational efficiency and productivity, enhanced risk management and controls, and better combatting of fraud and money laundering."*

**- DP5/22 - Artificial Intelligence and Machine Learning (Bank of England)<sup>7</sup>**

Furthermore, global standard setters such as the FATF<sup>8</sup> also highlight the opportunities of new technologies for AML/CFT purposes stating that “technology can facilitate data collection, processing and analysis and help actors identify and manage money laundering and terrorist financing risks more effectively and closer to real time.”



*“Transaction monitoring using AI and machine learning tools may allow regulated entities to carry out traditional functions with greater speed, accuracy and efficiency (provided the machine is adequately and accurately trained).*

*These models are useful for filtering the cases that require additional investigation. The use of new technologies for monitoring purposes should, for the most part, continue to be integrated with the broader monitoring systems which include an element of human analysis for specific alerts or areas of higher risk. These systems must also improve their degree of explainability and auditability in order to fully comply with the majority of supervisory requirements.”*

**- FATF, Opportunities and Challenges of New Technologies for AML/CFT**

However, AI is not without threat. Criminals are also leveraging AI to scale fraud, automate money laundering schemes, and bypass AFC controls, such as identity verification. Deepfake technologies, synthetic IDs, and AI-generated documents present real and growing challenges, as outlined in the UK’s most recent National Risk Assessment (NRA)<sup>9</sup> and the European Banking Authority’s (EBA) Opinion on Money Laundering and Terrorist Financing risks<sup>10</sup>. As such, the latter report states that financial institutions face challenges in detecting sophisticated AI-driven attacks that are increasing in both volume and velocity. Addressing these threats will require a combination of advanced technologies and specialised expertise. Firms must therefore be cautious, not only in how they use AI, but also in how they defend against its misuse.

## The 'Human' Touch - The Context Engine

Whilst firms are adopting AI at different paces and for different use cases, the need for human expertise remains essential. Experienced investigators bring contextual judgement, cultural awareness, and a deeper understanding of intent and typologies in a way that a machine often cannot interpret. This qualitative insight is critical in distinguishing suspicious activity from legitimate anomalies.

Human oversight is also vital in the development and training of AI systems. Without it, AI can inherit and perpetuate bias:



### Data bias

When the data only represents certain regions or customer demographics, leading the model to unfairly target those groups.



### Label bias

When historical decisions which could be shaped by human prejudice are used to inform the model causing it to perpetuate and even amplify any biases.



### Sampling bias

When the model is trained only on a small or narrow population which is not representative of the overall customer base.

A diverse team of TM investigators, data scientists, and financial crime experts must work together to ensure models are trained, validated, and governed effectively. When AI is fed rich customer, device and behavioural context, it can drive risk-relevant outcomes.

Human-in-the-loop frameworks allow for the continuous review and calibration of AI decisions, mitigating risk and enhancing explainability. AI excels at scaling insights but needs human input to guide, challenge, and validate its outcomes.

## The Power of the 'And' – The Hybrid Solution

The question is not “human or machine” but “how best can these be combined?”. The most effective TM models are hybrid by design. Rather than choosing between automation and human insight, firms should focus on how best to integrate the two. A hybrid approach can offer several benefits:

### ✔ Prioritised alerts

AI can filter out low-risk cases, allowing analysts to focus on high-value, complex tasks.

### ✔ Continuous improvements

Feedback loops between human decisions and AI systems help retrain models improving accuracy over time.



### ✓ Risk-based monitoring

Supports a proportionate approach, delivering prioritised alerts, reduced false positives, and improved typology detection while ensuring human oversight for regulatory comfort.

---

### ✓ Regulatory assurance

Maintains human oversight for governance, accountability, and auditability.

Ultimately, a well-governed hybrid approach enables firms to scale their monitoring capabilities in a way that can be effective, proportionate, and aligned with regulatory expectations.

## Solving the Dilemma

A successful hybrid model depends on robust governance to ensure effectiveness, accountability, and regulatory compliance. Key components include:

### ✓ Model risk management

Ongoing validation and testing to detect drift, degradation, or unexpected outputs.

---

### ✓ Bias detection

Regular audits/reviews to identify and correct discriminatory patterns that could compromise fairness or lead to over alerting on certain customer or transaction segments.

---

### ✓ Explainability frameworks

Ensuring decisions can be interpreted and justified to auditors, customers, and regulators. This should be supported by robust documentation to clearly and transparently highlight any AI-driven decisions.

---

### ✓ Human-in-the-loop approach

Maintaining human judgement at key decision points, reducing the reliance on automation.

---

### ✓ Auditability

Documenting data inputs, model decisions, and rationale for accountability.

Transparency and explainability is particularly important when it comes to the use of AI from a regulatory perspective. The FCA has raised concerns around “black box” models that lack transparency<sup>11</sup>. Under its AI regulatory principles, firms must be able to explain how AI systems arrive at decisions—particularly in high-risk areas like TM. This is not only a compliance issue, but also a matter of public trust and ethical responsibility.



Governance frameworks should be embedded from the outset and maintained throughout the AI lifecycle. They must be flexible enough to evolve with changing technology and threat landscapes. Regulators are pushing for the safe adoption of AI while simultaneously raising the bar on governance, explainability, and oversight.



The FATF has outlined both the opportunities AI presents in strengthening AML/CFT frameworks and the guardrails needed to mitigate its risks. In the UK, the FCA's AI Live Testing and Supercharged Sandbox initiatives are creating controlled environments where firms can trial AI models under direct regulatory visibility. Meanwhile, in the EU, new obligations for general-purpose AI will take effect from August 2025, with additional requirements for high-risk systems phased in between 2026 and 2027. The direction of travel is clear: transaction monitoring must be treated as a governed, high-accountability system.



*"Governance – AI may also pose some novel challenges for governance, especially where the technology is used to facilitate autonomous decision-making and may limit or even potentially eliminate human judgement and oversight from decisions. Some of the data and model issues can also have implications for governance. For example, a lack of explainability or transparency in some AI models may mean extra care or actions are needed to ensure full accountability and sufficient oversight."*

**- DP5/22 - Artificial Intelligence and Machine Learning<sup>12</sup>**

To make this shift, organisations must take practical steps: adopt AI incrementally and purposefully, invest in upskilling analysts to work alongside intelligent systems, and establish strong governance to monitor performance, mitigate bias, and maintain transparency. By embedding this augmented intelligence model into their compliance frameworks, firms can build a transaction monitoring function that is not only more efficient and accurate, but also resilient in the face of tomorrow's threats.


# Implementing a Hybrid Model:

## Practical steps


Transitioning to a hybrid TM model involves several key stages:

- 1. Assess readiness** Review existing transaction monitoring systems, data infrastructure, and workforce capabilities. Decisions should be made on whether AI can be used to enhance existing technologies and whether you are required to onboard a third party vendor which offers built in AI transaction monitoring solutions.
- 2. Start small** The business should decide why the use of AI will help support their transaction monitoring framework and what pain points require addressing. The firm should trial AI modules to determine its use case (e.g. triage, alert prioritisation).
- 3. Invest in data quality** AI is only as good as the data it learns from. You should ensure all data-sets are up to date and that any customer relationship management (CRM) or payment systems tools are collecting information and feeding into the appropriate data fields as required.
- 4. Train your people** Upskill analysts in AI literacy to bridge human-machine collaboration. The AML/CTF compliance function should be supported by an interdisciplinary team including financial crime SMEs, data scientists and engineers who can help build a well trained AI model.
- 5. Ensure governance** Establish frameworks for oversight, model explainability, and bias mitigation. There should be continuous monitoring of the tool from the outset and throughout the AI lifecycle. This is to avoid any concerns with model drift over time and ensuring the model is trained appropriately.
- 6. Engage stakeholders** Whether, this be senior leadership, the board, your auditors or regulators, be transparent about your AI approach, especially in audit and reporting processes. It should be clearly documented and understood where and how the use of AI is supporting a process.
- 7. Iterate and scale** Learn from pilots, refine, and expand across broader data sets. Building the AI model is a continuous process and should be continually tested across diverse scenarios.


These steps ensure that AI is deployed in a way that complements, rather than disrupts, existing controls—strengthening both effectiveness and regulatory confidence.




*"Today, real-time transaction monitoring serves as the backbone of our compliance strategy. Week by week, we have expanded the features we use, especially on the AI front. We've seen returns on investment from day one."*




**Angela Cavendish**  
Fraud & Financial Crime Manager






*"By integrating an AI-native compliance platform, we have improved our fraud detection and AML monitoring capabilities, helping us identify and mitigate risks proactively while maintaining high compliance standards."*



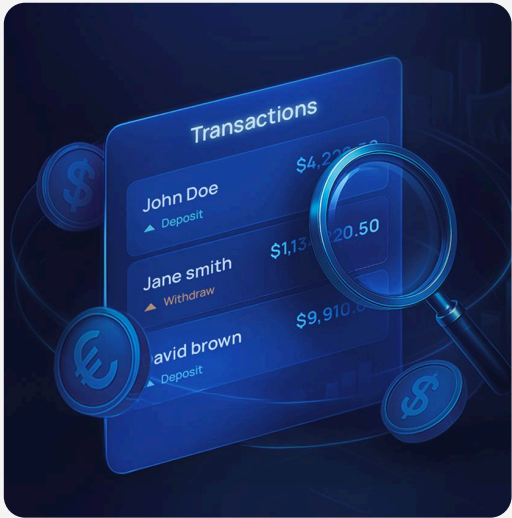
**Tom Jennings**  
CEO



# The Co-pilots of Transaction Monitoring

As financial crime grows in sophistication and scale, the limitations of relying solely on either AI or human judgement in transaction monitoring are increasingly clear. AI offers unparalleled speed, scale, and analytical power, but lacks the contextual awareness and ethical reasoning that experienced human investigators bring to the table. Conversely, human-led processes struggle to keep pace with evolving risks and volumes without technological augmentation.

The future of effective transaction monitoring lies not in choosing between the two, but in combining their strengths through a hybrid approach. Deployed well, this model enables financial institutions to reduce false positives, prioritise high-risk alerts, and adapt dynamically to emerging typologies, while maintaining the human oversight necessary to satisfy regulatory expectations and ensure accountability. Artificial intelligence and human insight are not competitors - they are co-pilots. And only together can they meet the rising standard for financial crime detection in a complex and fast-moving world.



# Sources

1. [SWIFT](#)
2. [FATF, Opportunities and Challenges of New Technologies for AML/CFT](#)
3. [Opinion of the European Banking Authority on money laundering and terrorist financing risks affecting the EU's financial sector](#)
4. [Artificial Intelligence \(AI\) update – further to the Government's response to the AI White Paper | FCA](#)
5. [A pro-innovation approach to AI regulation: government response - GOV.UK](#)
6. [Implementing the UK's AI regulatory principles: initial guidance for regulators - GOV.UK](#)
7. [DP5/22 - Artificial Intelligence and Machine Learning | Bank of England](#)
8. [FATF, Opportunities and Challenges of New Technologies for AML/CFT](#)
9. [National risk assessment of money laundering and terrorist financing 2025 - GOV.UK](#)
10. [Opinion of the European Banking Authority on money laundering and terrorist financing risks affecting the EU's financial sector](#)
11. [Machine learning in UK financial services - FCA 2019](#)
12. [Bank of England](#)





Flagright is an AI-native, no-code platform for transaction monitoring and AML compliance. It enables financial institutions to centralize detection, investigation, and reporting of suspicious activity, streamlining regulatory workflows and strengthening financial crime controls. By replacing fragmented systems, Flagright helps reduce false positives by 93% and lower compliance costs by 80%, thereby setting the modern standard for financial crime compliance.

[Get in touch here](#)



FINTRAIL is a global consultancy passionate about combating financial crime. We've worked with over 100 global leading banks, FinTechs, other financial institutions, RegTechs, startups, venture capital firms and governments to implement industry-leading approaches to combat money laundering and other financial crimes. With significant hands-on experience in the US and UK, we help you prepare, assure, and fortify your controls to meet evolving regulatory requirements.

[Get in touch here](#)