WHY AML NEEDS AI: DEBUNKING THE MYTHS

White Paper

RESISTANT.AI

FINTRAIL

Contents

Introduction

Artificial intelligence (AI) is fast becoming a hugely powerful tool in fighting financial crime. Increasingly recognised and supported by regulators and adopted by financial institutions, AI has progressed from theory and research to successful real-world use. Surveys in the UK show AI is increasingly being adopted by both established financial services firms and newer FinTech companies[1]. It is used in many areas of risk management, from credit risk to claims management, but its adoption for anti-financial crime has had a slower start, even though the potential benefits are clear.

This paper will focus on the use of AI in transaction monitoring, one of the most rewarding use cases. It strengthens the anti-financial crime function by overcoming inefficient processes, identifying more incidents of suspicious behaviour, promoting quicker decision making, adapting in real-time, and facilitating a firm's scalability. Automated processes can reduce the burden of managing extensive rule sets and processing false alerts. AI algorithms quickly process huge volumes of information to establish networks among vast data sets and detect connections, networks and patterns that are essentially undetectable to human analysts.

Amongst practitioners there is a prevailing image of AI as a cutting-edge, highly sophisticated and desirable tool but one that can be inaccessibly complex and daunting. This perception means many small or midsize companies may shy away from implementing AI-enhanced transaction monitoring tools. Despite being prime targets for criminals seeking to exploit unsophisticated controls, newer and smaller firms often regard AI as an unnecessary or unobtainable luxury. But are they right, or are they being put off by unfortunate misconceptions? Is there a more innovative route to harnessing the power of AI for better transaction monitoring?

This white paper will highlight critical opportunities for FinTechs interested in exploring how AI can improve their transaction monitoring processes in a practical, complementary, and unobtrusive way. It uses interviews with compliance experts from the FinTech sector to discuss how AI can be applied to the fight against financial crime, dispelling common myths surrounding its applicability and providing practical guidance for achieving concrete outcomes. Ultimately, it will argue that AI is a growth-enabling tool that can identify more instances of money laundering and fraud and provide huge efficiency gains for FinTechs of any size.

[1]Bank of England and FCA, 'Artificial Intelligence and Machine Learning', October 2022

Debunking perceived barriers to adopting AI

Myth 1:

"My firm is too small; AI is only accessible to large institutions"

Even when recognising potential benefits, a key concern for small and midsize FinTechs is the accessibility and practicality of AI solutions. While larger firms boast more generous budgets and bigger client bases and transaction volumes to justify complex and expensive solutions, FinTechs in growth mode often feel their operations don't warrant investment into AI. They prefer to stick to traditional rules-based systems because of their comparative simplicity - they don't require extensive technical or analytical expertise, and firms can either purchase off-the-shelf solutions or develop their own monitoring capabilities in-house.

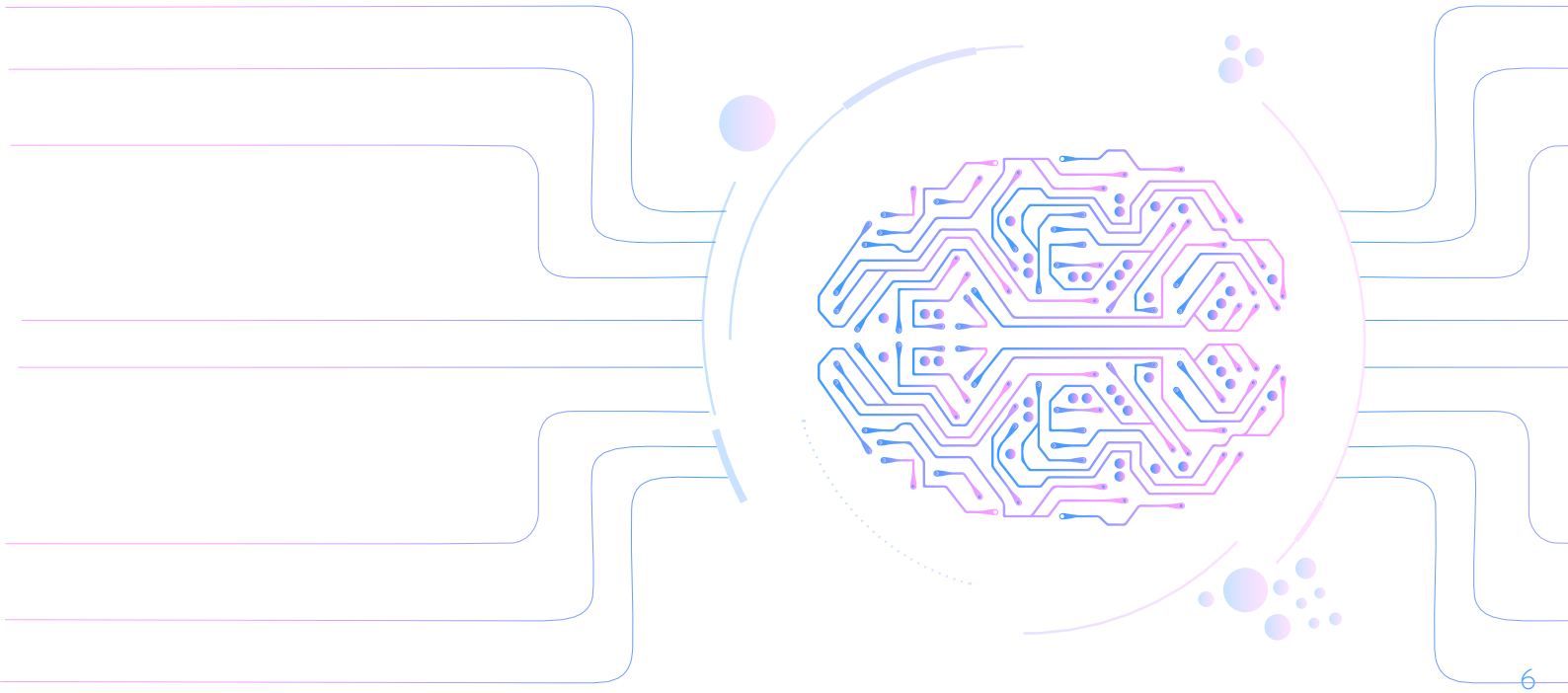
Not all AI-powered transaction monitoring solutions are created equal.

Some need significant resources for implementation and have prerequisites in terms of data points, interfaces, and architecture. Acquiring AI for transaction monitoring often means a replatforming exercise, with the AI elements being bundled with pre-built case management tools and rules engines that are not easily customisable and may not be best suited for a firm's particular needs. However, other AI solutions work with already-used tools, whether self-built or vendor-provided, to augment and optimise a firm's existing capabilities. This can be an attractive alternative to a full solution replacement for FinTechs who are outgrowing their existing transaction monitoring platforms, but want to *enhance* rather than *replace* what they currently have, retaining elements that they are happy with such as case management and reporting tools.

Relying on rules-based systems that are 'good enough for now' not only forfeits the benefits of AI, but carries a number of risks. Firstly, unsophisticated controls are why criminals target new or small FinTechs in the first place, preying on vulnerabilities and loopholes to conduct significant damage before compliance teams can react. Nefarious actors can easily deceive legacy rules-based systems by purposely avoiding set thresholds and adopting complex transaction patterns. Secondly, rules-based systems are inherently reactive rather than proactive. Rules are by necessity constructed based on past experience or best practices, both of which struggle to keep pace with fast-evolving financial crime techniques. AI enables firms to identify novel fraud and money laundering behaviours as they occur, meaning those firms can act immediately before too much damage is done. Consequently, AI-enhanced transaction monitoring can limit a FinTech's overall exposure to financial crime.

Implementing an AI-powered transaction monitoring tool at an early stage of growth holds immense advantages. Setting good foundations from the start is much easier than upgrading later, once it is incontrovertible that an existing system is not working as it should or is no longer fit for purpose. While rules-based systems can be low-tech and easy to understand, they rely on manual input and ongoing management that can quickly become time-consuming.

AI tools can be an asset for scaling businesses, enabling them to be comfortable with expanding their operations and taking on new risks by making them better able to mitigate them.



Myth 2:

"We don't have enough quality data"

A lack of data is a pressing issue for new start-ups or small to midsize FinTechs. Data and AI are inseparable, with data analytics drawing insights that are used to continuously learn and improve. Many believe having a near-perfect, complete, and thoroughly labelled dataset is a prerequisite for AI adoption. However, even firms with limited data features or a lack of historical, labelled data can benefit from implementing AI. After all, *any* organisation will say their data quality could be improved - this is far from a unique issue for small firms. Indeed, FinTechs are perhaps better placed than larger organisations to incorporate additional data over time due to their agile nature. Getting started with AI should not be viewed as an impossible quest just because data is a little imperfect.

Instead of viewing limited data as a barrier and waiting for the 'perfect data moment', making the most of existing data through innovative analytical approaches such as ensemble modelling can overcome data limitation issues. An ensemble approach combines multiple AI techniques to better leverage existing data, ultimately requiring less labelled training data and overcoming the issues many smaller firms experience when getting started. Solutions can be deployed and refined as the system gradually ingests data and learns over time, improving synchronously with the firm's growth.

Popular data quality misconceptions

✖ **You need labelled data.** Some AI techniques, like anomaly detection, rely on examining behaviours as transactions are processed. No labelled data is necessary.

✖ **You need to build your own models immediately.** You can use readily available detection method libraries that are modelled on specific patterns such as muling and layering.

✖ **Your existing data.** Relying less on complex features in favour of imperfect, simpler models that work in unison, you can combine multiple AI techniques to leverage the data you do have with ensemble-model AI.

Recognising the limitations of rules-based monitoring systems, many firms supplement them by engaging in typology-sharing initiatives to try and keep ahead of new trends. While opportunities for collaboration are essential, and have been explicitly recognised this year by the Wolfsberg Group[2], they are gravely limited by privacy restrictions. Partnerships are essentially reactive - at best, powerful reflections on previous instances of financial crime. For a firm to be proactive and forward-thinking, it must embrace more sophisticated technology-led controls.

Ultimately, there is no practical substitute for a FinTech's own individual data. Their unique real-life datasets are complex, varied, and crucially inform the detection of financial crime risk. For firms that wish to grow, augmenting current processes with AI tools sets the foundation for better data collection and enhanced capability. As FinTechs look ahead, the only way to defend against real-time attacks, protect the profitability of their organisation and effectively tackle financial crime is by adopting data-driven AI solutions and beginning the journey to data optimisation and improvement.

[2] The Wolfsberg Group, 'Effectiveness through Collaboration', June 2022

Myth 3:

"It's a black box; the regulator won't like it"

Let's be clear - the idea that supervisory bodies don't like AI is a myth. Some have issued encouraging statements, some have adopted a technologically-neutral stance, but none have publicly discouraged the use of AI. However, it is true that with increasingly stringent regulations around AI (e.g. the European Union's proposed Artificial Intelligence Act[3] or the US's Blueprint for an AI Bill of Rights[4]), the need for explainability remains critical. Many people assume that AI solutions are inherently opaque black boxes which are incomprehensible to regulators and thus treated with hostility. In fact, regulators widely recognise AI tools as important, as evidenced by regulator-led initiatives in the US, the EU and Singapore[5], to promote innovation including the use of AI in regulatory technology.

Just as criminals and fraudsters use new technologies to commit financial crimes, financial institutions are increasingly expected to include technology and innovation in their anti-financial crime arsenals. The global money laundering and terrorist financing watchdog, the Financial Action Task Force (FATF) has explicitly recognised technological innovation as holding great potential, with AI and machine learning tools allowing firms "to carry out traditional functions with greater speed, accuracy, and efficiency[6]". As firms must prove to regulators that their systems are compliant and effective, the deficiencies of rules-based monitoring systems become more apparent. Additionally, the European Banking Federation has called on firms to ensure that the future of AML involves innovative technologies that add to human experts' judgement in assessing complex criminal networks, not rely on dated and conventional methods[7].

Despite these endorsements, many FinTechs remain worried and shy away from adopting AI. But a better approach would be to focus on explainable AI, which means choosing accessible solutions and documenting decision-making processes. One particularly explainable AI solution is ensemble modelling,

[3] European Union, 'Artificial Intelligence Act', April 2021

[4] The White House, 'Blueprint for an AI Bill of Human Rights', October 2022

[5] FinCEN, European Commission, Monetary Authority of Singapore

[6] FATF, 'Opportunities and Challenges of New Technologies for AML/CFT', July 2021

[7] EBF, 'Demystifying AI for AML', October 2021

which uses a combination of models to get the best possible result. The type of data used for making decisions relating to fraud or money laundering scenarios can often be high-dimensional with multiple features involved. Ensemble modelling uses a diverse set of relatively simple models and their predictive accuracies to obtain a consensus-based decision. This compares with alternative approaches which use a single, more complex model to reach a decision. The ensemble modelling approach helps with explainability given that each of the simpler constituent models is inherently easier to explain.

AI adoption should start with creating a robust and effective data mapping process and project management framework, meaningfully involving all stakeholders and logging and detailing decisions. This makes it easier to explain to internal and external stakeholders how AI tools integrate with existing controls, what they are designed to do, and how they are performing. As one Head of Risk and Compliance notes, explainability should be separated into two categories: explaining controls and explaining AI itself. Good AI providers will be able to clearly describe how their tool works to their customers, even if they are not AI or data specialists, enabling them in turn to explain it to their own stakeholders and to regulators.

> *It's important to tailor your explanations of systems and rules to your audience - for example an internal vs. external stakeholder, an AI / ML technical specialist vs. someone non-technical. We have different types of documentation covering how our systems are built, how they work, and what behaviour the different rules are monitoring for.*
>
> ***Billy Pinder, Head of Transaction Monitoring, CurrencyCloud***

At its crux, understanding AI should not be contingent on having experts in large data science teams providing jargon-filled explanations. Different levels of knowledge are necessary across the firm to promote an inclusive technology culture. While some AI solutions may be intimidatingly complicated, painting all AI tools with a broad brush misses critical distinctions. Outsourcing AI capabilities to trusted partners can help companies scale safely without waiting until they are big enough to hire data scientists in-house. Outsourced solutions can be explainable-by-design, meaning compliance officers can clearly describe and discuss their processes with internal and external stakeholders, backed by external expert technical support.

To ensure your financial crime detection processes are explainable, look for AI providers that:

- Engage from both a technical and business point of view to articulate how AI can be used and where it will add value.
- Offer a flexible approach to integrating with existing capabilities.
- Are flexible enough to work with the data you have.
- Offer ongoing support with model management, compliance and scaling AI as your business grows.
- Give you direct access to technical teams for support and questions.
- Provide continuously tuned and automatically updated models to avoid resource-intensive model retraining.

Myth 4:

"AI is too expensive"

At the heart of any business decision is accounting for the bottom line. While AI-powered monitoring tools undoubtedly drive operational efficiencies and reduce costs in the long run, there is often a significant initial cost. Weighing up the upfront cost against return on investment (ROI) can be off-putting for FinTechs with a limited compliance budget. Finding an AI product that uses a software-as-a-service model and supplements existing tools rather than replacing them is a good solution for firms with limited initial resources. Because you don't need to hire an army of data scientists, you can reap the benefits of AI with minimised upfront and ongoing costs. Outsourcing this requirement for expertise to a trusted external partner can reduce costs overall via a variety of value levers.

The gains from adopting AI-powered monitoring tools go beyond immediate enhanced efficiency. AI holds the key to scalability, allowing firms to increase their business operations without hiring more people. The prevailing reputation of compliance tools as a financial drain can finally be transformed into that of a growth enabler, offering a healthy ROI. Compliance leaders can advocate for these solutions internally in line with broader business and financial goals.

Commercial use case

One of the most pressing challenges for FinTechs of any size is grappling with rising fraud. With UK victims losing a massive £1.3 billion to fraudsters in 2021 alone, FinTechs are increasingly forced to consider the financial impact of fraud on their business operations, in terms of both the value of fraudulent transactions and the compliance resource burden. AI solutions can identify more cases of fraud as they happen and consistently adapt to emerging trends, minimising losses as well as protecting customers and the firm's reputation.

[7] UK Fraud, 'Annual Fraud Report 2022'

AI tools in transaction monitoring save you the need to hire analysts in both transaction monitoring and customer due diligence, becoming a big cost saving point.

Kseniia Kutyreva, Head of Risk and Compliance, FINOM

In addition to helping with costs during lean economic times, AI tools are critical in hiring and retaining talent during 'employee markets'. By minimising low-value repetitive work, AI makes AML jobs more fulfilling which translates to better retention, more engagement, and a healthy company culture. No matter the economic conditions, using AI to streamline investigations, reduce repetitive workflows and automate where possible can minimise costs and ensure talent is focused on high-value problems requiring human analytical skills. Analysts that are endlessly bombarded with false alerts may start rejecting alerts on autopilot, increasing their chances of missing genuinely suspicious transactions.

Adopting AI technology keeps an existing team curious, allowing them to constantly develop and improve their skills, and fosters a healthier work environment.

Smart people want to work on hard problems. How to employ AI and technology in financial crime compliance is a hard (but exciting) problem. Our people are motivated by the challenges of using AI alongside traditional methods.

Billy Pinder, Head of Transaction Monitoring, CurrencyCloud

Myth 5:

"It's too much work to change our whole programme"

Completely overhauling an existing process is an expensive and time-consuming ordeal. Acquiring AI-powered transaction monitoring solutions can often mean adopting an entirely new platform that replaces what is already there - including the good bits. This means FinTechs need to factor in the time and money associated with implementation, configuration, and extensive team training. Understandably, lean and growing FinTech teams are reluctant to spend money and efforts on replacing something that is already running, even if not optimally.

Instead of completely overhauling a rules-based transaction monitoring programme, it will often be better to augment rather than replace it. Instead of discarding what already works, AI-powered AML tools that focus on strengthening and refinement allow for an easier and more practical transition. This aligns with the views of the Head of Compliance at a scaling FinTech, who views AI adoption as a process rather than a one-off task: "AI is something that you need to work on continuously, as part of a journey."

FinTechs can get better value from existing investments in technology by enhancing the products they already work with, rather than disrupting their business operations entirely and wasting previous efforts. Additionally, it is easier for FinTechs to explain to regulators how their controls work, when any new tools are overlaid on familiar rules-based systems.

What now?

Next steps for FinTechs

Financial crime will persist as long as bad actors continue to use innovative technological advancements to bypass or deceive controls. Small or midsize FinTechs are often the target of malicious actors seeking to circumvent unsophisticated controls, cutting into the firm's bottom line and creating negative reputational impacts.

In the transaction monitoring space, AI tools have been shown to improve efficiency and effectiveness and are endorsed by regulators and industry leaders alike. AI is being used by financial institutions right now, in real-world scenarios, to mitigate multiple types of risk. The posited advantages are no longer theoretical; they have been proven in real life. Moreover, some firms have a significant track record of delivering AI-powered solutions to the private sector, and are using learnings and insights from many years of practical experience in using AI to fight related forms of criminal activity.

This white paper demonstrates that not all AI tools are created equal. When it comes to AI adoption, finding a suitable solution for your firm is a huge part of the battle. FinTechs should actively consider adopting AI tools to enhance, augment, and refine their existing systems — using AI providers flexible enough to serve smaller or growing FinTechs as well as more complex organisations.

Getting started

- **Assess your resources for any change programme in the short to mid-term.** Adopting an AI solution isn't as simple as picking a tool from a list, buying it and turning it on - as with any meaningful improvement, it will require some bandwidth to get it right.

- **Conduct a review of your existing processes and outputs.** This will give you a base for comparison and inform your case for purchasing a new tool. Many data points may be helpful here (i.e. the number and percentage of false positive alerts, SLAs for processing alerts, QA results, employee turnover, etc.)

- **Investigate where else in your business AI is used or being considered.** There may be synergies or existing internal expertise you can leverage.

- **Ask around.** Excellent compliance practice is not a competitive advantage. Other firms may be happy to share their experiences, give advice on implementing an AI solution, or recommend the best provider.

- **Look under the hood.** Remember, not all AI solutions are created equal. Thoroughly assess how well the provider can explain their solution by asking difficult questions, getting granular on how a tool would integrate with your existing systems, insist on understanding how AI will add value to your business, and finding out what ongoing support is available beyond the point of purchase.

- **Prepare a realistic project plan for senior management and other stakeholders.** Your plan should include a clear cost and benefit analysis, the resources necessary for each stage of selection and implementation, the likely time frames, and which teams need to be involved.

Appendix

An introduction to Resistant AI

Effective transaction monitoring requires balancing customer experience with accurate risk detection and using limited resources in a shifting regulatory landscape. Excessive false positives and significant investigative costs are the norm, but are hard to reconcile with a real-time business context. Incessant innovation by criminals and constant compliance scrutiny lead to escalating complexity in risk detection rulesets. But there is a way to respond without wholesale replacement of existing solutions.

Transaction Forensics

Resistant AI is the data-driven, AI-powered solution that augments existing AML transaction monitoring systems to make the transition to a more effective, risk-driven approach to detecting financial crime. Instead of adding further, complex rulesets in response to escalating regulatory requirements, cut out the noise generated by inefficient rules, boost your AML compliance and reduce costs. Adding practical, explainable AI to your transaction monitoring – using a powerful ensemble of machine learning techniques in tandem with existing rules – you can prioritise alerts to reduce workload, uncover previously-hidden risks and detect clusters of related events.

We would love to show you how together we can outpace money launderers and combat financial crime. Contact us today and a member of our team will answer any questions you may have about how to stop money laundering. Read more here.

Winning approach

Did you know our data-driven, anomaly detection approach to transaction monitoring has been recognized for a second time after winning the PwC-sponsored ACAMS hackathon challenge in Las Vegas, following our win at ACAMS Hollywood last March? Read more

Our key priority is the flexibility of the provider. We found that many providers were really set on using their own dashboards and workflow. And they're really not flexible in terms of incorporating new data. For instance, if we wanted to add a new data point that we found, like data from a news article or statistic on a country, incorporating that into the transaction monitoring process would require raising a product request, which then gets analysed by the provider, which then gets placed on a roadmap. ***Resistant AI is really perfect because they do not insist on you using their own workflow. They just provide you with the data.***

Kseniia Kutyreva, Head of Risk and Compliance, FINOM

The main driver for working with Resistant AI to optimise our existing transaction monitoring rules was to reduce false positive alerts without losing true positives. We took a collaborative approach to the optimisation exercise and have seen a 30% reduction in the number of alerts generated per week. This is really helping the team focus on more meaningful alerts.

Billy Pinder, Head of Transaction Monitoring, CurrencyCloud

Co-authored by

RESISTANT.AI FINTRAIL