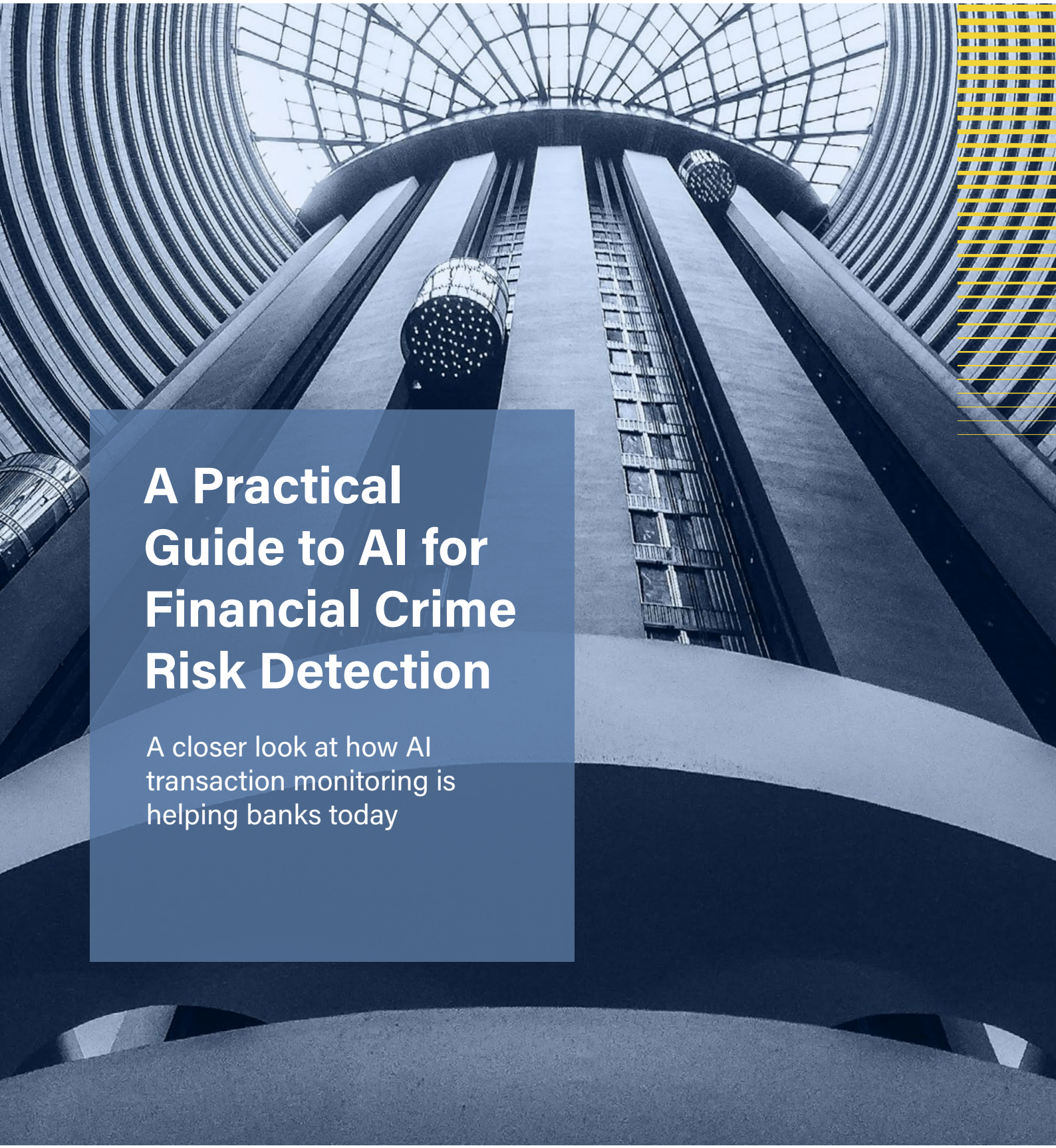
ComplyAdvantage.com

RESISTANT.AI



A Practical Guide to AI for Financial Crime Risk Detection

A closer look at how AI transaction monitoring is helping banks today

2022

COMPLY ADVANTAGE®

Contents

Thinking differently about financial crime risk detection

Between the volatility of global financial markets and turbulent political issues like the war in Ukraine, the risk landscape for financial crime has never been harder to predict.

At the same time, the financial services industry has itself been going through dramatic change with innovations like new payment methods, digital wallets and cryptocurrencies.

Add to that the constant stream of new regulatory requirements and it's clear why so many banks are struggling to cope with the challenge of monitoring their customer's transactions.

The teams responsible for detecting financial crime are burning out. Up against a ruthlessly dynamic risk landscape with rulesets proliferating beyond control, they're forced to monitor alert logs that generate so much noise they make actual risks harder to detect.

Banks *need* a new approach to detecting financial crime.

From defenders to hunters

Current strategies for managing financial crime aren't working. What's needed is a pre-emptive approach.

In anti-money laundering (AML), pre-emptive risk management refers to the principle that banks must proactively identify and seek out the financial crime threats they face.

With the rise of AI-based AML solutions, it's become clear that a reactive, rules-based approach that relies on historical data and guidance from law enforcement is no longer sufficient.

Pre-emptive risk management is also fast becoming a regulatory requirement. Regulators expect banks to use the vast quantities of data at their disposal and the innovative RegTech solutions available on the market to identify new risks.

This is part of a wider focus on advanced analytics, data sharing and global public-private partnerships across major jurisdictions.

The Financial Action Task Force's (FATF) 2021 report on 'Opportunities and Challenges of New Technologies for AML/CFT' highlights the role new technologies play in making AML measures faster, cheaper, and more effective.

The FATF's report cites the use of AI to solve 'complex problems' - the effective detection of criminal behavior is one such problem.

> "Artificial intelligence (AI) and machine learning (ML) technology-based solutions... can strengthen ongoing monitoring and reporting of suspicious transactions. These solutions can automatically monitor, process, and analyze suspicious transactions and other illicit activity, distinguishing it from normal activity in real-time, whilst reducing the need for initial, front-line human review."

Programs designed to proactively detect financial crime aren't just better placed to avoid negative headlines from regulatory enforcement and costly infrastructure overhauls when new regulations are introduced.

They also help banks minimize the number of customers falsely flagged due to outdated systems and data.

This paper will go beyond industry buzzwords to explore organizations' specific and practical use of AI in their financial crime risk detection programs, focusing specifically on use cases related to transaction monitoring.

The use of AI in transaction monitoring

AI has long been identified as a key tool to support banks in predicting, detecting, and deterring financial crime more effectively than traditional approaches. Indeed, the latest deep learning-inspired AI has been in the market for a decade and is readily available for organizations to exploit.

How AI helps

One of the defining features of AI is its ability to quickly process and make sense of large volumes of information and detect patterns in data. This is why it can add tremendous value to transaction monitoring.

For the purpose of AML transaction monitoring, machine learning is the subset of AI that can help organizations make a step change in their detection.

When applied effectively, machine learning enables regulated entities to detect known risks with greater speed and accuracy while also increasing their detection of novel, previously unknown criminal activities, the 'unknown unknowns.'

Another key benefit of AI is its ability to establish networks across seemingly unrelated data sets. For example, large webs of account holders may be known associates or connected beneficial owners, use related contact information, reuse the same names with slight variations, or even exhibit the same behaviors in the same areas.

Similarly, cases involving high-profile persons – whether PEPs or high-ranking executives – provide interesting use cases for network analysis, given the high-risk relationships these individuals may have with friends, family, and business partners.

Machine learning can help banks of all sizes

When banks consider machine learning, many see data as a barrier, particularly in the case of early-stage organizations. Many believe that only large, established firms can use machine learning because they have large volumes of labeled, historic data.

However, machine learning can add value to organizations of all sizes by enabling them to gain more leverage from their available data.

Two of the most well-known approaches are supervised and unsupervised machine learning though there are several techniques including graph analytics, deep neural networks, segmentation, behavioral analysis, and numerous others.

The challenge is that organizations can be overwhelmed by the choices they have to navigate in order to find the most suitable solution to a multi-dimensional problem like financial crime detection.

Have your cake and eat it too: The ensemble approach

The ensemble approach combines an assortment of machine learning techniques. One of the many benefits of this approach, when compared to a single model approach, is how it uses data.

Ensemble models use a powerful blend of classic machine learning and simple models, which require less labeled training data to put such models into production use.

This allows organizations to combine the predictive accuracy of multiple smaller models to build the optimal decision. Each model analyzes different components of transactions and can hone in on a specific aspect of the task at hand, such as identifying behaviors indicative of money laundering or fraud.

For example, one model might focus on the size of transactions. Another might pertain to its location. A different model could examine which specific actors are involved in the transaction.

The combination of each of the results of those models is what surfaces instances of criminal behavior. This approach to detection provides a fully informed, robust, consensus approach to decision-making.

> "When our imperfect judgments are aggregated in the right way, our collective intelligence is often excellent."
>
> **- James Surowiecki,** Author

Ensemble models can be applied to transaction monitoring to support organizations in managing their existing financial crime risks more efficiently and effectively while also allowing a more forward-looking approach by detecting novel, previously unseen behaviors and evolving threats.

For transaction monitoring, specific benefits of applying AI include:

- The ability to automatically triage alerts to enable you to automate first pass alert remediation, freeing up analysts' time to focus on high-risk and more challenging cases
- You gain more effective tuning, with greater power to improve and adjust parameters and thresholds of underlying rules
- You uncover more bad actors. Weak evidence related to one person alone may not lead to an escalation. However, with AI, banks can leverage weak correlates in their data pools to identify and disrupt clusters of criminal activity
- You can identify true actors working behind the scenes by using identity clustering to seek out hidden relationships
- You get greater insights and explainability around the reasons for an alert being generated

Evolving regulatory expectations

Through draft legislation, presentations and new initiatives, regulators globally are making clear that AI will be integral to financial crime risk detection programs going forward.

Monitoring and understanding regulators' approach to AI now will help firms better anticipate future regulatory requirements. It will also enable them to explain any AI-based transaction monitoring use case in alignment with their regulator's specific priorities.

This section explores statements made by leading regulators indicating how AI will be deployed in regulatory frameworks.

United States

- In January 2022, FinCEN acting director Himamauli Das gave a speech to the American Bankers Association (ABA), highlighting the Anti-Money Laundering Act of 2020 (AMLA) as a watershed moment in the history of U.S. AML/CFT regulations. The AMLA helped to modernize the country's AML/CFT regime. Today, Das explained, "FinCEN is helping transform our nation's AML/CFT regime from post-9/11 to post-pandemic; from al Qaida to AI and digital assets."

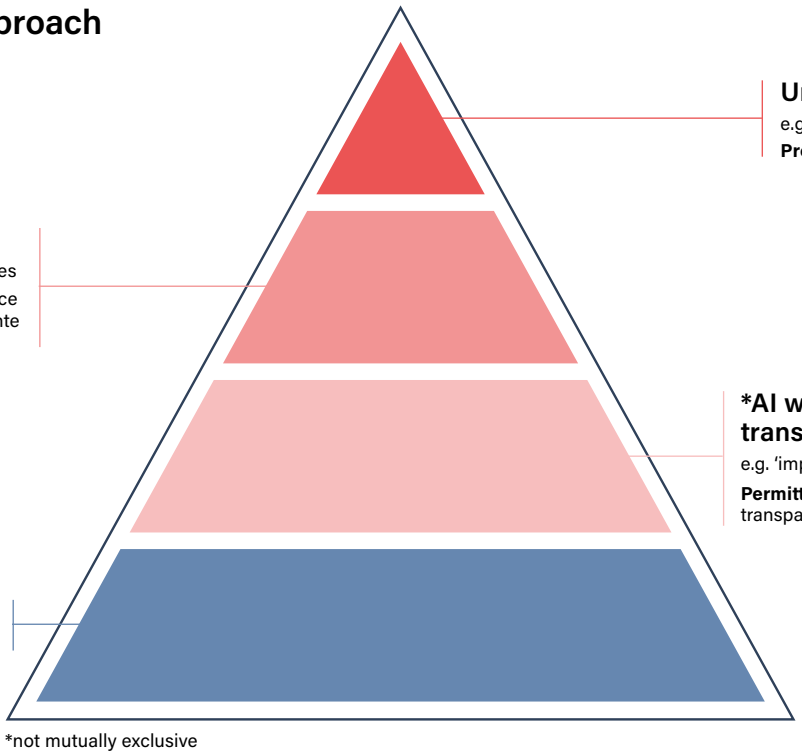
- In May 2022, the House of Representatives Committee on Financial Services held a hearing titled "Keeping Up with the Codes – Using AI for Effective RegTech". The hearing discussed the use of AI in supervisory and regulatory technology (referred to as SupTech and RegTech, respectively). It explored the rising need for artificial intelligence, discussing the importance of proper development to mitigate risks such as dataset pollution by bad actors, data privacy, and the transmission of bias from humans into AI systems.

- US regulators have also moved from encouraging guidance into concrete action. In June 2022, the government requested public input on plans to implement a consistent no-action letter process in the future. Through this, it hopes to remove some of the barriers to compliance innovation firms have experienced in the past. FinCEN is also working to implement collaboration tools and events, such as sandboxes, Innovation Hours, and international TechSprints to encourage RegTech innovation.

European Union

- In March 2022 the European Commission issued a Call for Tenders in an initiative to launch a pan-European regulatory sandbox focused on blockchain. It also partnered with Spain in June 2022 to initiate a pilot of the EU's first AI-focused regulatory sandbox. In general, the initiative is with individual EU states to implement sandboxes in line with their national priorities and EU regulatory guidelines. This may change, however, as the European Council has recently announced the new Anti-Money Laundering Authority (AMLA), creating hope for future focus on AI/ML in the field.
- In April 2021, the European Commission proposed the far-reaching Artificial Intelligence Act (AIA), the first attempt to legislate on AI internationally and across sectors by a major regulator. Now working its way through the legislative process, the Act would establish a framework for AI/ML development seated firmly in human rights protections.
- The AIA intends to create parameters allowing artificial intelligence to develop in ways that are good for society by controlling for its most significant risks. The regulation aims to be as technology-neutral as possible, defining AI as a "set of techniques" to allow for future developments. It also aims to avoid cumbersome over-regulation of the industry while still protecting fundamental human rights. To accomplish this, it creates a risk pyramid within AI techniques that would focus regulation only on the highest-risk areas of the industry.

A risk-based approach to regulation



*not mutually exclusive

Source: European Commission

United Kingdom

- In 2019, the Financial Conduct Authority (FCA) released a report with the Bank of England titled "Machine Learning in UK Financial Services." The report analyzed the results of research into the use of advanced AI technologies in the financial sector. Survey respondents found ML capabilities improve AML/CFT compliance and enhance efforts to objectively stop financial crime while providing better insights than traditional tools. Moreover, these benefits were expected to increase in the coming years. In 2021, the FCA commissioned another report by the Alan Turing Institute, which further validated these findings and, with the input of FCA team members, explained in-depth how AI can improve the fight against financial crime.
- In 2022, the FCA released a final report on the AI/ML Public-Private Forum held between 2020 and 2021. Besides discussing at length the general use of AI in the financial sector, it emphasized the need for regulators to find a way to share certain "relevant data" – such as "which Suspicious Activity Reports were genuine and which were not" – to ensure machine learning is fully effective for use in AML/CFT applications.

Singapore

- Singapore has been a consistent leader in the exploration of AI for the financial sector. In 2019, MAS announced the launch of announced Veritas, a public-private framework to help the industry develop responsible AI-driven solutions. Risk scoring and fraud detection were among the multi-phased consortium's first areas of focus.
- MAS also currently offers a Regulatory Technology Grant to support the development of innovative risk management tools among FIs it regulates. It also hosts a regulatory sandbox. Both these programs are part of a larger FinTech and Innovation initiative seeking to provide broad support for Singaporean FinTech innovation. Most recently, the agency announced Project Ellipse, a prototype for cutting-edge SupTech intended to use machine learning to boost regulators' effectiveness in combatting global financial crime.

Next steps

The use of AI/ML within regulatory frameworks generally - and transaction monitoring specifically - is no longer just theoretical: countries are beginning to adopt it to improve supervision and support its development in the private sphere. Artificial intelligence as a tool against financial crime will likely become standard in the coming years. As a result, firms should particularly monitor regulations in the jurisdictions in which they operate for consultations, guidance, regulations, and sandbox-style initiatives that enable them to de-risk innovation and proof of concept projects.

Governance and explainability in AI

There is a shared view among regulators and practitioners that AI can be a game changer when fighting financial crime. However, the successful adoption of innovative technology, such as AI, is still thin on the ground. There are several reasons for this limited adoption, including a lack of understanding and practical know-how.

Further challenges to adopting AI are transparency and explainability, as seen as the ability to understand and trust the results and output created by AI.

You don't have to start from scratch with governance

Regulators encourage "banks to consider, evaluate, and, where appropriate, responsibly implement innovative approaches to meet their AML compliance obligations, in order to further strengthen the financial system against illicit financial activity." AI is one such innovation that is encouraged. There is an expectation from regulators that AI models should be effective, explainable, up-to-date, and adapted to the specific risks and needs of each customer. Model governance is a way to ensure these expectations are met.

Model governance is crucial to the safe and responsible adoption of AI. It ensures accountability and establishes a framework and the necessary oversight for an organization's use of AI.

Model governance is not new, and organizations are further along than they think. They don't need to start from scratch. Existing governance and model risk management frameworks provide a solid foundation and a good starting point for AI, as the objectives are the same: To demonstrate that appropriate oversight and controls are in place for safe and responsible use of technology used to make decisions.

These frameworks can be adapted to cover AI models and should help organizations to understand and effectively manage the specific risks relating to the use of AI. Governance frameworks should cover the entire lifecycle of AI from model development to ongoing use and provide evidence that effective oversight and accountability are in place.

Maintaining strong model governance and risk management frameworks from the get-go will put organizations in good stead for internal and external reviews.

The need for explainability

AI is often referred to as a `black box.' This is due to the belief that with AI, we can observe the inputs and outputs but cannot explain the mechanism that connects one to the other. Explainability plays a key role in dispelling this belief.

The need for explainability is not unique to AI, it is critical across all controls. Explainability is a basic condition to enable trust and ensure responsible use of technologies. As per the FATF's definition, explainability means that technology-based solutions or systems are, "capable of being explained, understood, and accounted for."

A key element of the FATF's definition is that explainability should "provide adequate understanding of how solutions work and produce their results." The word adequate is an important one, as there is often concern from organizations adopting new technology solutions, particularly those that make use of AI, on what amounts to adequate. In this context, there is a need for clearer and more comprehensive regulatory expectations.

The FATF and global regulators have on many occasions highlighted that they are 'technology neutral,' implying organizations should have an adequate understanding of how the technology solutions underpinning their financial crime control framework work and produce outcomes, whether they are AI-driven or otherwise.

Goals of explainability

Explainability is often spoken about in the context of the regulator, but the goal of explainability is more than just appeasing regulators. It is about maximizing investigator effectiveness.

The importance of explainability for financial crime investigators cannot be underestimated. Explainability is critical for effective investigation and to enable users to make the best use of systems.

Explainability is imperative for investigators' decision-making process. It is important for users to have transparency over the factors that determine outcomes so investigators can make informed decisions and do so in a fast and effective manner.

For instance, if an investigator does not know why a model generated an alert on a transaction, they won't know where to begin their investigation, resulting in a highly inefficient process.

Suppose the model not only flags transactional activity as warranting further investigation but also comes with a human-readable explanation as to why the transaction was flagged. In that case, the investigator can do their work more efficiently and effectively. This explanation becomes critical when transactions are blocked, as staff need to understand and explain the reason for blocking or holding a customer payment.

'Computer says no' is unlikely to cut it!

AI that promotes explainability

Interpretability is regularly used in the context of explainability. It is argued that, like FATF's 'adequate understanding,' 'sufficient interpretability' is what should be expected from AI. That is, a stakeholder can comprehend the main drivers of a model-driven decision. Interpretability captures the idea that one of the most useful and practical ways to explain a decision is often simply to articulate its main drivers.

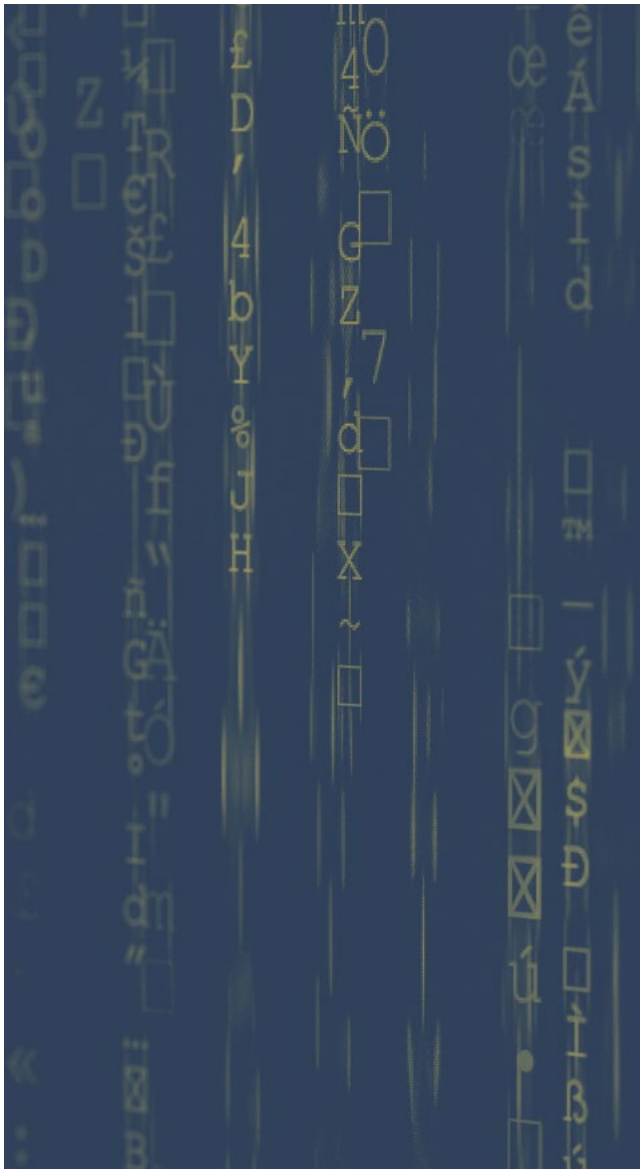
This is why interpretability by design proves truly useful and reinforces the benefits of the ensemble model approach, where the creation of a simpler model from the outset supports more explainable outputs, as discussed in previous sections.

In an ensemble, individual models assess just one factor in a transaction. This allows interpretability of their outputs as well as full explainability with text. With ensembles, it is possible to pinpoint a micro-segment, for example, the size of the transaction. This enables the use of text next to the output, which highlights that the transaction size is too high for the economic sector of this company.

5 steps to deploying AI in transaction monitoring

Once AML compliance teams understand where and how AI can support their work, the next step is to define a real use case. Inevitably, this will initially focus on a specific area of the compliance function. As this paper has shown, transaction monitoring and the ensemble approach provides a powerful use case firms can start with today.

So, where should firms get started? The five-step process below is based on interviews with ComplyAdvantage/ Resistant AI customers. Customers turned to AI because they felt financial crime prevention remained too manual and focused on identifying known risks. They recognized that their data could be used to identify new and unexpected insights.



1. Define core objectives

It may sound obvious, but setting clear, realistic goals for scoping a potential solution will ensure the deployment runs more smoothly. The benefits of the investment can also be more easily assessed. Examples include:

- Alert prioritization, enabling analysts to focus on the transactions that pose the highest level of risk
- Reducing the reliance on manual processes by automating alert triage in transaction monitoring
- Improving rule reviews to more effectively reduce false positives while ensuring true positive matches can be actioned quickly
- Identify unusual and anomalous patterns of behavior, and the ability to uncover hidden relationships between entities

2. Review regulator expectations and guidance

Firms should consider the regulatory landscape in which they operate, especially if an AI-based process is replacing, rather than supplementing, an existing, more manual operation.

Regulators are agnostic about the technology that firms use. They also believe that AI should not mean responsibilities are transferred from humans to machines. Accountability remains with compliance officers. However, there is a growing recognition of the value AI can bring to financial crime risk detection systems.

In a recent report exploring the opportunities and challenges of new technologies for AML/CFT, the Financial Action Task Force (FATF) examined the power of AI to help firms analyze and respond to criminal threats with automated speed and accuracy. This is because machine learning can be used to train computer systems to "learn from data" without the need for extensive human intervention. FATF reports will likely help inform how individual regulators think about innovations in AML/CFT.

3. Set realistic implementation timelines

While it's important to plan ahead and allow for contingencies when deploying AI-based AML/CFT solutions, the implementation process doesn't have to be costly and time-consuming. With appropriate planning, AI can be accessible to banks.

Valentina Butera, Head of AML and AFC Operations at Holvi, a leading digital bank, explained that "it's hard to implement AI that isn't just reinforcing your existing thinking." As Butera highlights, in areas like anomaly detection,

> "AI can be a powerful way to examine previously unknown risks and novel events. Delivering such use cases requires specialist knowledge and skills."

4. Identify day-to-day users

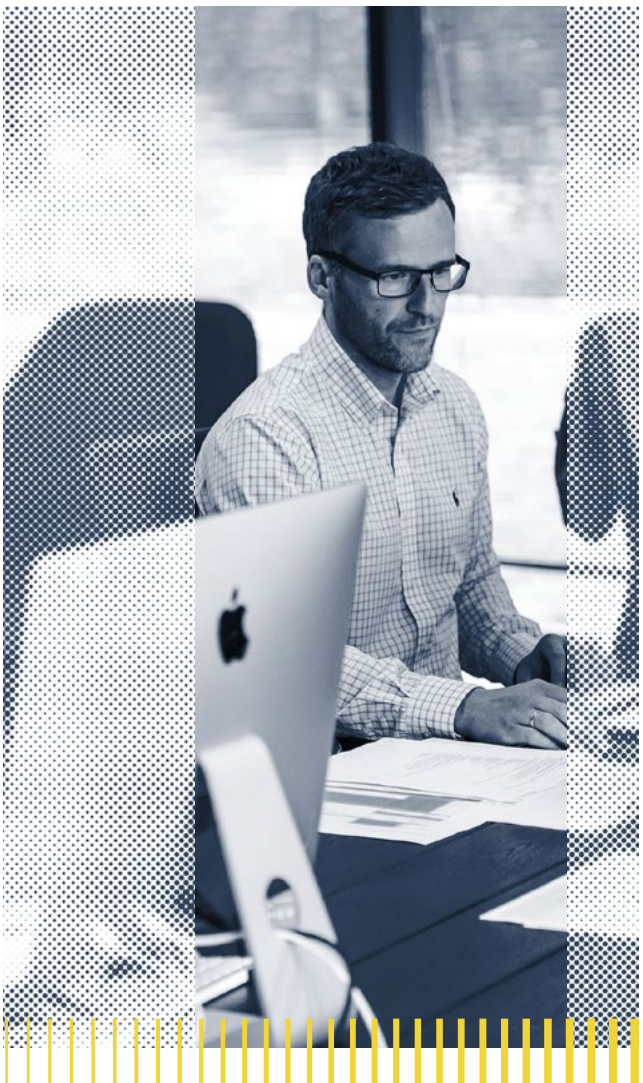
Based on the selected use case, compliance leaders should also identify who in their team will interface with the new solution. Doing this early on ensures appropriate team members can be involved in the implementation process, allowing them to ask questions about the opportunities - and limitations - that come with AI. They will also better understand the methodologies behind the AI system's recommendations.

It's also vital to arrange formal training, usually organized by the vendor(s) involved in implementation. Ongoing training, and regularly scheduled reviews in the first weeks the solution is live, will also be critical.

5. Map implementation to growth goals

Finally, firms should consider how AI-based AML will support their growth plans. "Effectiveness and efficacy are key for scaling. We can't grow our team every time we grow our customer base," explains Butera. Her observation reflects a challenge felt by many compliance teams. More customers will likely mean more false positives and, therefore, a higher number of alerts to manage. Questions to consider include:

- How can AI support prioritization work as volumes scale?
- What strategic hires would best complement the benefits of the AI-based use case?
- Where will the effectiveness of AI-based automation be more helpful and challenging as customer volumes grow?



Solution Overview: Smart Alerts

Smart Alerts can overlay an existing AML/CFT transaction monitoring system, enhancing it without requiring a total overhaul. It can be a cost-effective and low-risk way for firms to upgrade legacy tools, resulting in improved efficiency, quicker decision-making, and more comprehensive compliance infrastructure.

There are two core components to the Smart Alerts solution, each with its own specific use case.

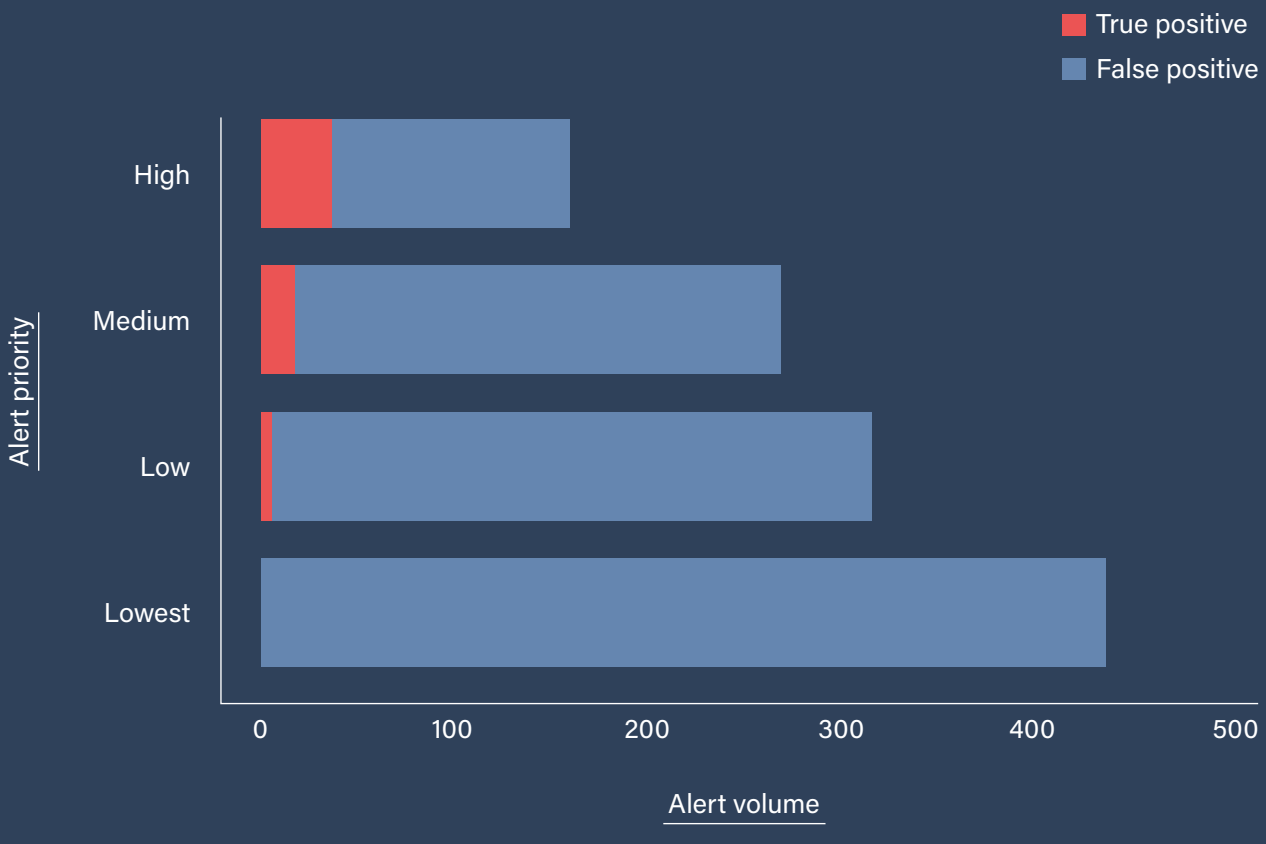
Alert Prioritization

Smart Alerts will interface with firms' existing transaction monitoring systems, using a supervised learning algorithm to classify alerts as high, medium, or low-risk. As analysts process alerts, the supervised learning algorithm uses its feedback to fine-tune its algorithm, improving its suggestions continually.

Alert prioritization allows experienced analysts to focus their time on high-priority alerts. The highest risk alerts rise to the top, allowing analysts to concentrate on activity most likely to lead to a SAR. Meanwhile, low-risk alerts are either bulk-remediated or can be reviewed by more junior analysts. This capability is especially powerful for firms working to remediate a large backlog of alerts. In one use case, Smart Alerts reduced analysts' work by 33%. This in turn improves overall workflow efficiency, which is critical for helping firms to scale effectively.

As an AI-based model, with integrated feedback loops, its performance will continue to improve over time.

Alert Prioritisation



New Detections

Smart Alerts can also detect new suspicious activity that traditional systems would overlook. It analyzes diverse signals to detect hidden relationships and complex webs of activity, such as money muling or layering. It also reviews anomalous activity, such as odd-amount transactions or behavior that doesn't fit a given segment's typical profile. Put together, this use of novel data insights can powerfully enhance risk investigation and reporting.

Despite its complexity, the solution provides clear, documented reasons for its risk detection decisions. This explainability gives analysts a confident basis for continued research, ensuring a clear audit trail is in place.

There are a number of use cases for Smart Alerts' new detection capabilities:

- Identity clustering, allowing teams to track customers who use multiple accounts to subvert rules and regulations (see diagram below)
- Anomaly detection using sophisticated segmentation, allowing firms to track not only overall outlier transactions but also transactions that are outliers within their segment
- Statistical and numerical analysis, allowing the identification of a series or sequences of transactions with unusual numerical patterns
- Advanced, industry-specific models for use across blockchain, payments, neo-banks, and more

Identity Clustering

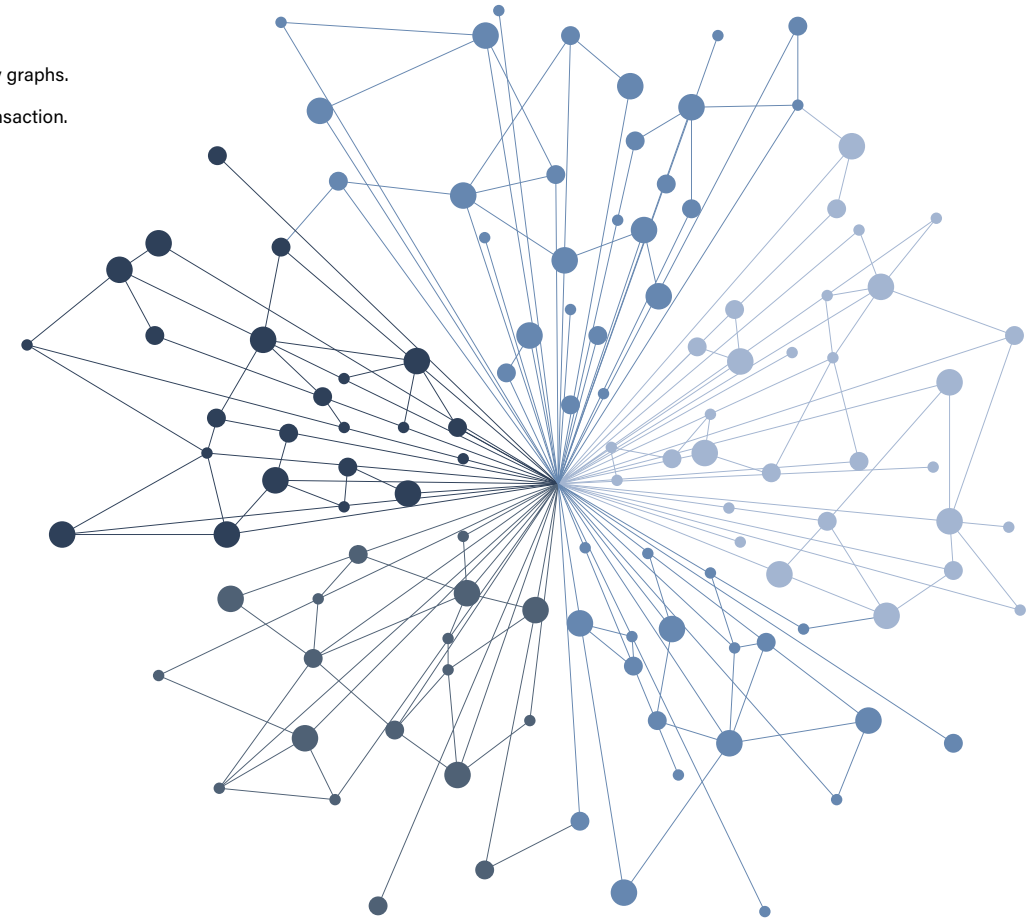
Connected components of identity graphs.

Each node represents a single transaction.

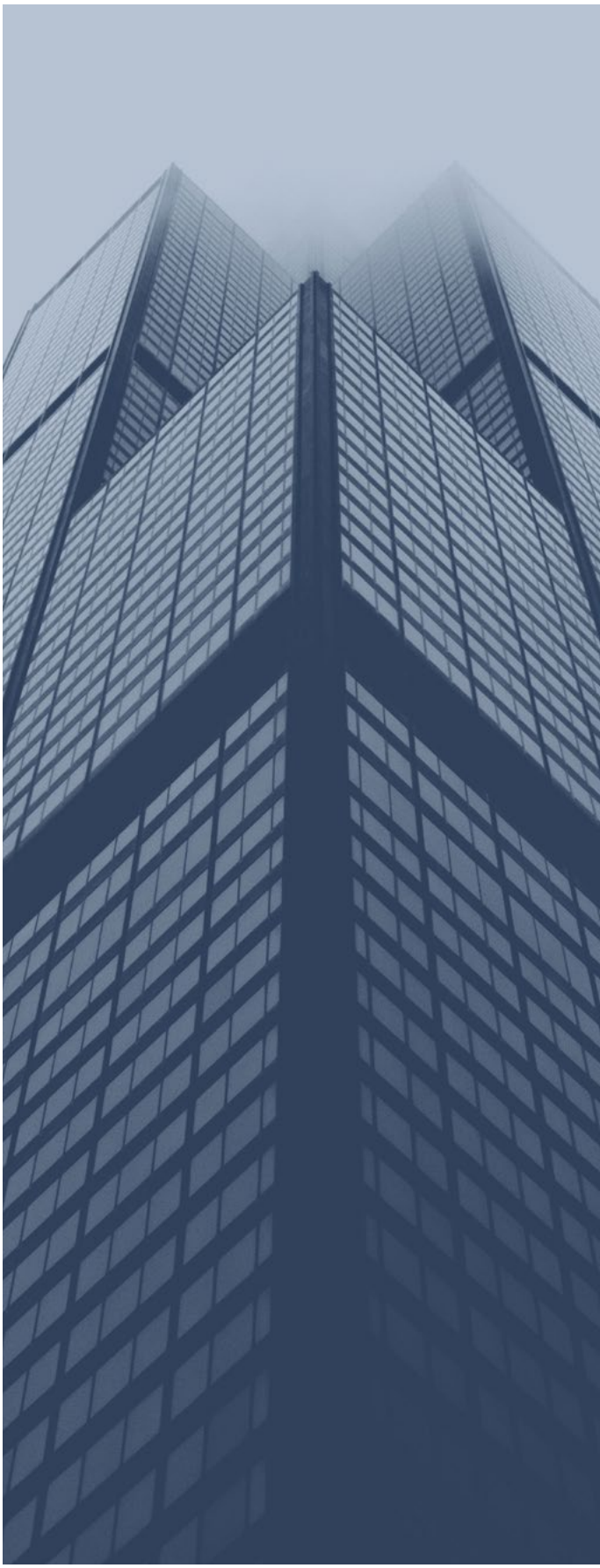
Cluster example:

53 unique identities containing:

- 39 names
- 49 phone numbers
- 16 emails
- 14 IP addresses



Conclusion: Evolving compliance



For years, compliance teams have known that legacy AML software and processes have not met the financial crime challenges faced by their organizations.

Rigid rules and tick boxes may capture egregious behavior but they miss much of the complexity involved in illicit activity. They also cannot see the bigger picture and broader connections between entities and people necessary to help law enforcement eliminate criminal behavior root and branch.

The tools and technologies now exist for banks to meet this moment. 'AI' is no longer simply a buzzword - it's an umbrella for many actionable programs that firms can implement today. Regulators worldwide recognize this and will likely soon ensure AML regulations reflect the innovations available to firms in their jurisdictions.

Now, the most significant problem is how to focus an AI-driven effort. With many possible use cases, firms can quickly become overwhelmed with the possibilities and inadvertently choose inertia. Firms can use this paper's sentiments, use cases, and proof points to avoid this trap, identify a coherent proof of concept, and expand their efforts using AI.

Can AI put your bank on the front foot?

To find out more about a realistic path to gaining value from AI, talk to us about your bank's challenges with financial crime risk detection.

Get in touch

About Resistant AI

Founded in 2019, Resistant AI uses AI and machine learning to provide identity forensic solutions that protect automated financial services from fraud and manipulation, including customer onboarding, AML and existing fraud detection systems. The Resistant AI founding team has a deep background in machine learning, artificial intelligence and computer security with more than 15 years of experience applying AI in the computer security domain. Backed by GV (formerly Google Ventures), Index Ventures, Credo Ventures, Seedcamp and several angel investors specializing in financial technology and security, Resistant AI is headquartered in Prague with offices in London and New York.

Visit resistant.ai to learn more.

About ComplyAdvantage

ComplyAdvantage is the financial industry's leading source of AI-driven financial crime risk data and detection technology. ComplyAdvantage's mission is to neutralize the risk of money laundering, terrorist financing, corruption, and other financial crime. More than 500 enterprises in 75 countries rely on ComplyAdvantage to understand the risk of who they're doing business with through the world's only global, real-time database of people and companies. The company actively identifies tens of thousands of risk events from millions of structured and unstructured data points every single day. ComplyAdvantage has four global hubs located in New York, London, Singapore and Cluj-Napoca and is backed by Ontario Teachers', Index Ventures and Balderton Capital. Learn more at:

complyadvantage.com

Get in Touch

EMEA
London

+44 20 7834 0252
Demo Request

AMER
New York

+1 (646) 844 0841
Demo Request

APAC
Singapore

+65 6304 3069
Demo Request

For details on the source materials used in this guide, please visit complyadvantage.com/insights