AI for Anti-Money Laundering

Improve accuracy in detecting anti-money laundering activity while reducing wasted effort in investigating false alerts.

C3.ai

01

The Challenges of Anti-Money Laundering

Enforcement actions and penalties for non-compliance with anti-money laundering (AML) regulations are on the rise. Fines for AML, data privacy and MiFID have risen 27% in 2020. US regulators have historically been the toughest enforcers of AML rules, but in 2020 APAC overtook the US in the value of enforcement actions and there has been an increased focus on penalizing individuals, rather than just financial institutions. At the same time banks are likely to get squeezed even further if the US implements a proposal to lower the suspicious transaction threshold from $3,000 to $250. This will force banks to significantly increase their investment in AML operations to manage the growing number of investigative cases. Compliance teams are already fighting to keep up with the increasing volume while under immense cost pressure and saddled with outdated technology.

At the same time bad actors are employing an increasingly diverse set of strategies to stay ahead of regulators and compliance departments. This includes shifting activity towards the non-bank financial sector or taking advantage of the anonymity that comes with digital currencies, virtual assets, custodian wallets, and pre-paid cards.

If the situation was not complex enough, the COVID-19 pandemic has wreaked havoc on banks' transaction monitoring and related AML compliance capabilities. Security protocols and the associated infrastructure for banks was developed for a world where compliance and AML operations were run from within the physical confines of a bank's office, not for the current necessity of employees accessing servers remotely from their homes.

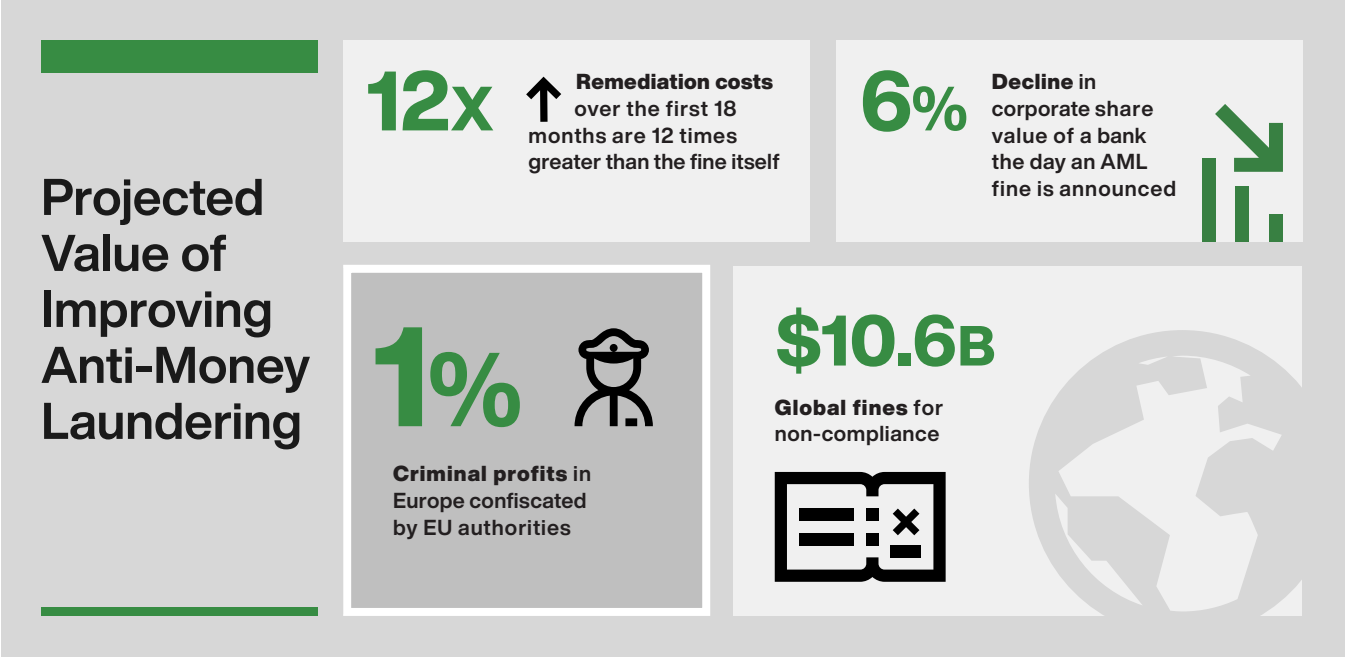


Figure 1: *Projected value of improving Anti-Money Laundering*[1,2,3]

Traditional rules-based AML software create an excessive amount of alerts that require review and disposition by compliance investigators. Not only are these investigations painfully long, require navigating the multiple systems of a typical bank, but are often fruitless, with over 95% of the alerts proving to be false positives.

Regulatory demands for increased money-laundering scrutiny are on the rise and so are the associated costs of AML operations. In response, banks need to reimagine their AML operations with greater automation and apply a different approach for identifying and investigating suspicious activity.

1. How Europe Can Fight Anti-Money Laundering, July 2020
2. Financial Institution Fines, Fenergo, 2020
3. Anti-Money Laundering Controls Failing to Detect Terrorist Cartels and Sanctioned States March 2018

02

Adjust Your Mindset to Better Handle These New Challenges

Compliance organizations are rightfully concerned about the required growth of their analyst teams and IT infrastructure to handle the increasing regulatory burden. The use of strictly traditional systems and tools would likely lead down that path, raising the "cost of doing business" potentially to values high enough to justify exiting certain markets or jurisdictions. But the past need not be prologue, and savvy managers are becoming aware of fundamental truths that take advantage of recent technological innovations in artificial intelligence and distributed computing:

1. **Next-generation know your customer (KYC) and AML operations** do not focus on discrete and siloed client risks (e.g., transaction monitoring and sanctions screening), but rather consider a dynamic risk-based view of each client and their context within the broader ecosystem.

2. **There is no tradeoff or incompatibility** between artificial intelligence / machine learning (AI/ML) techniques and regulator-ready auditability and evidence packages.

3. **Advanced system architectures** exist to bring together as much data as possible to train algorithms while not compromising on security practices, exposing private information, or breaching local jurisdictional rules.

A Holistic View of a Client

Financial institutions have built entire compliance divisions over time that adhere to outdated software constraints. This has led to fragmentation of client data across different teams, business processes, and systems, such as KYC, CDD, EDD, sanction screening, negative news screening, transaction monitoring, and others, which make it difficult or even impossible to generate a true, unified view of a client's risk profile.

Instead, these systems should generate the true business and compliance need: a holistic and dynamic view of a client based on all available internal and external data.

Combine data from transactions, sources and uses of funds, sanction lists, news articles across multiple languages, and CRM information. Keep the data image current with near real time updates. Maintain the network graph of all related parties, associations, and money flows. Adding additional intelligence layers through advanced rules or AI/ML will then yield tremendous business operational benefits and significant risk reduction.

Artificial Intelligence is Now Transparent

Financial crimes regulators have high reporting standards and place a significant burden on financial institutions to provide clear, transparent and traceable rationale for suspicious activity reports. These reporting standards have led financial institutions to develop rigid, rules-based systems to detect potentially suspicious behaviors. These systems rely on experts to define customer segments, scenarios or rules and thresholds. When thresholds are exceeded for the rules applied to a particular client, an alert is created. While rules-based systems may enable AML investigators to identify some illicit activity, they often have critical issues. First, bad actors can gain knowledge of common rules and craft their behavior to avoid detection. Furthermore, with rules-based systems, compliance and AML teams must manage an unsustainable number of false positive alerts. The rigidity of the rules does not allow these systems sufficient flexibility to learn behavioral patterns and accurately differentiate normal behavior for one client or segment from suspicious activity. For every productive or necessary investigation, investigation teams may disposition hundreds of superfluous alerts.

Yet these rules-based systems continue to be used despite the issues they create for AML teams. The continued use of rules-based systems is primarily due to the fact that rules are easy to tune, document and explain to regulators, and alerts produced by the system are straightforward and traceable to specific source data.

In the past few years enterprise artificial intelligence (AI) systems have made considerable progress in providing interpretability that will satisfy regulatory scrutiny. At this point, there should be no discernable difference in understanding "how" or "why" an alert was triggered between a rules-based system or one powered by advanced enterprise AI.

As AI systems continue to make progress in interpretability, traceability, data lineage and model management, adoption of AI-based AML modeling techniques is increasing. Additionally, AI-platforms that leverage these techniques can also provide advanced model management and monitoring capabilities that automatically track model performance and store and version key information about models, predictions, risk drivers, alerts and source data. These capabilities support all regulatory and audit-driven requirements for explainability and transparency.

Scale Out Your AI Systems Without Requiring New IT Projects Each Time

Traditional AML systems have often been implemented as standalone technology stacks for each line of business, in every region and regulatory jurisdiction. With this approach there are limited economies of scale for data processing and cross-jurisdictional learnings related to emerging money laundering schemes, or the identification of nested account relationships and global financial crime networks.

However, new advances in distributed computing make global deployments easier, and support combining key support unifying global, cross-border data across jurisdictions and implementations to uncover complex schemes and support more robust AI/ML model training.

Some financial institutions are centrally managing their AI models, deploying artifacts locally and enabling regional teams to retrain models based on local data. Such techniques are enabled by advanced system achitecutres that support global deployments in a much more cost effective way than individual, standalone IT implementations.

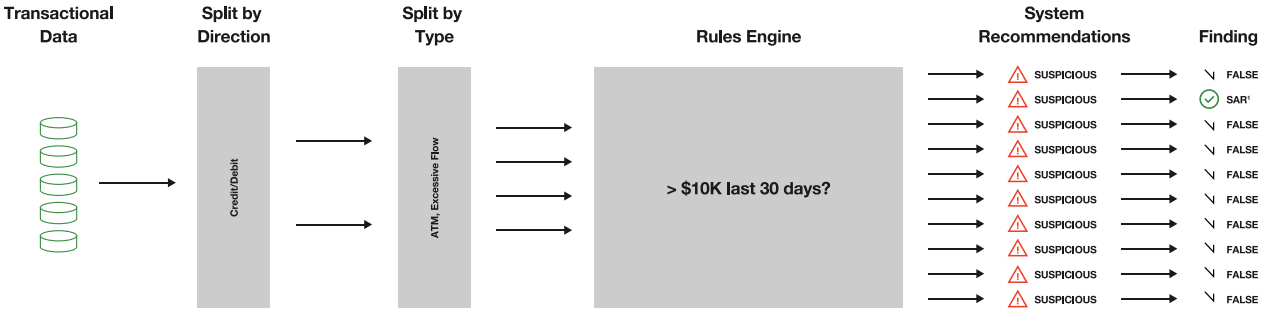
03

How to Start Improving Anti-Money Laundering with AI

Traditional rules-based systems are struggling to keep up with evolving regulations, money laundering strategies, and evermore new and complex scenarios. Enterprise AI and machine learning has the potential to efficiently parse through the massive volumes of data and accurately identify high-risk transactions and entities based on historical behavior, pre-analyzed patterns, and anomaly detection. For example, AI can detect emerging risk topologies, transactional anomalies, and new connections for established bad actors.

AI-based software solutions offer significant advantages over existing rules-based detection systems. Supervised machine learning models can be trained on past data and accurately identify, prioritize, and report suspicious activity, while simultaneously reducing the number of false positives. By augmenting the manual investigative process AI/ML models can significantly reduce the cost of AML operations while meeting the increased requirements being placed on banks by today's regulations. But to be successful in a real-world context, AI-based AML software systems need certain key capabilities.

Legacy Rules-Based Approach Produces a High Volume of False Positives



AI-Based Approach Yields High-Precision Identification of Suspicious Activity

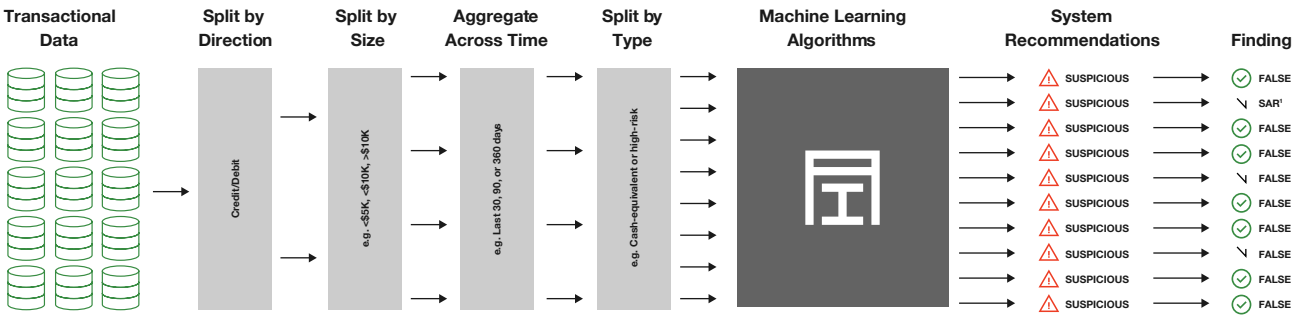


Figure 2: *Legacy rules-based approach vs. AI-based approach accuracy*

Incorporate Internal and External Data: The Advantages of AI-Based AML

Before applying any analytics, AI-based AML software applications need to deliver a universal view of the customer by integrating data from internal systems such as core banking, KYC, and transaction monitoring, as well as external sources like adverse media search results, sanctions, and politically exposed persons (PEP) lists. This unified view needs to work within a bank's current and ever-changing data and IT landscape where systems are evolving and being transitioned.

Monitor Transactions with Interpretable Machine Learning

Unlike traditional solutions that rely on rigid rules, AI-based AML software learns from past client behavior to detect suspicious activity and emerging risk typologies. An AI-based AML application should provide transparent, easy-to-interpret risk drivers for each money laundering risk score. Moreover, the AI/ML models should not be a black box, but rather should produce complete evidence packages and interpretable risk drivers to aid investigation officers in identifying suspicious transactions and entities while also understanding why they have been flagged as high-risk.

Enhance Investigator Productivity

AI-based AML software needs to understand and improve investigator workflows and aim to enhance their productivity. While providing transaction and entity risk scores based on AI models is a core capability, the software also needs to arm investigators with intelligent case recommendations, automated evidence packages, and advanced visualizations of key contextual case data, such as alerts, parties and counter-parties, accounts, transactions, and risk drivers.

Scale Across Enterprise

Global banks have to contend with varying data infrastructure, regulatory requirements, and AML practices across regions. AI-based AML software needs flexibility to meet these heterogenous situations across the globe, and AI models need to be easily configurable and flexible, enabling intelligent adjustments to changing regulations and money laundering strategies.

Enterprise AI for Anti-Money Laundering

Existing customer due diligence, transaction monitoring, and triaging solutions utilize simplistic analytics and rules-based models that struggle to identify complex money laundering typologies. Such systems tend to produce a large volume of false positives that quickly overwhelm AML operations without yielding fruitful results.

04

Comprehensive AI-Driven AML Operations

Improving Accuracy and Reducing the Cost of AML Operations

While every AI-driven AML operation is different, the general structure of such initiatives has the following steps:

1. Gather and Prepare Data

Developing accurate machine learning models for AML requires a wide breadth of internal and external data. In most organizations data are siloed across several disconnected systems. The first step is to unify and normalize the data into a single federated data image. The C3 AI Financial Services Data Model unifies and correlates all relevant financial services data for the purpose of modeling relevant patterns, behaviors, and relationships. Important data sources for AML machine learning models include client profile, KYC, transactions, and other data sources as illustrated in figure 3.

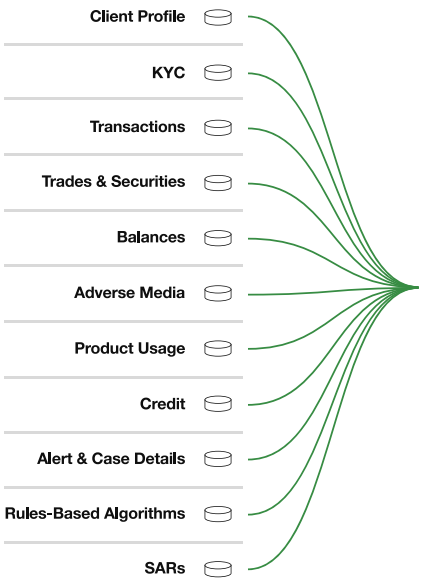


Figure 3: *C3 AI Financial Services Data Model unifies and correlates all relevant financial services data*

2. Create and Engineer Features

This step leverages the unified data and logical interactions of data elements to construct meaningful behavioral signals that "train" machine learning models. Time-based analytical signals are created as base machine learning model features from the unified data. The features are then parameterized by various attributes to construct complex patterns and correlations between signals across various time frames, transaction types, and other high-risk indicators.

		Parametric Modification					
Feature Class	**Feature Examples**	**Time Range**	**Attribute Type**	**Geographic Risk**	**Count/ Value**	**NLP**	**Related Parties**
Party	In depth profile of entity attributes, complexity of entity account structure, inconsistent entity information	✓	✓	✓	✓	✓	✓
Account	Age of oldest active account, number of account openings, changes to account information	✓	✓	✓	✓	✓	✓
Anomalous Aggregate Transactions	Total activity in period, historical and peer comparisons for beneficiary/ originator activity, cash-equivalent activity, unique counterparties, transaction sequence	✓	✓	✓	✓	✓	✓
Individual Transaction Flags	Transfers to/from high-risk destinations, Entity Domicile/ Nationality in high-risk country, high cross-border transaction volume	✓	✓	✓	✓	✓	✓
Segmentation + Graph	Proximity to high-risk party, peer group segmentation, transaction counterparty risk, similar accounts	✓	✓	✓	✓	✓	✓

Table 1: *Features are parameterized by various attributes to construct complex patterns and correlations between signals across various time frames, transaction types, and other high-risk indicators.*

These features map to familiar AML typologies and are used by machine learning models to learn complex behavioral patterns. The time-based nature of the features enables the models to replay history and observe how those patterns change over time as signals of potential money laundering activity. C3 AI AML includes over 5,000 time-based analytics that cover common AML typologies like structuring, rapid fund movements, and high-risk transactions.

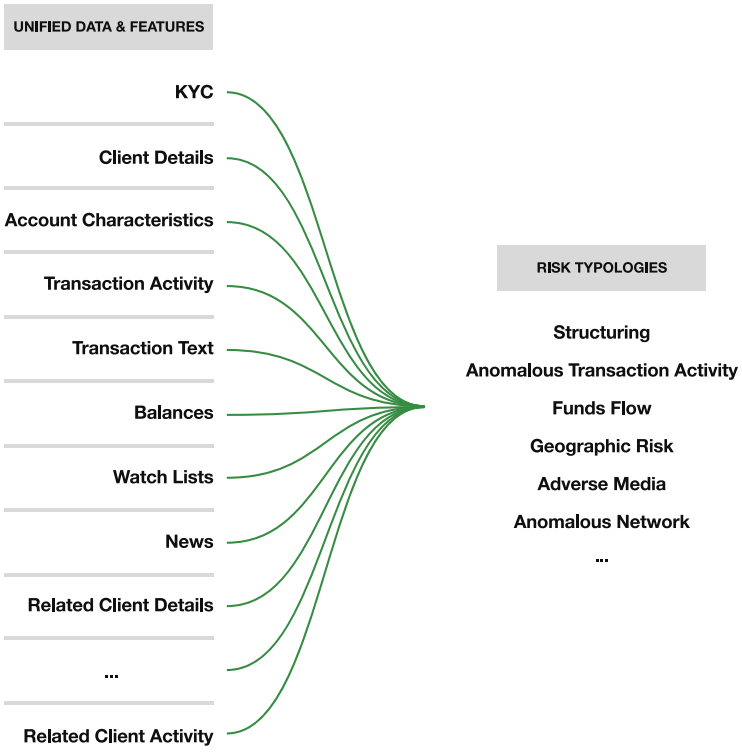


Figure 4: *Unified data and features map to familiar AML typologies and are used by machine learning models to learn complex behavioral patterns*

3. Train the ML Model

The now unified data and analytics form the input for a machine learning model framework that enables organizations to rapidly train models on their dataset so the models are tuned to the risk profile and behavior of that specific organization's clients. The breadth of the unified data and the ability to replay behavioral patterns using analytical signals vastly increases the accuracy of machine learning models.

It is imperative to have a machine learning model framework that supports a variety of model types, including:

- One model for an entire client population
- One model per client segment
- Supervised models (e.g., Random Forest, XGBoost, LightGBM, etc.)
- Unsupervised models

Certain model types may be better suited for certain AML problems. For example, one way that suspicious activity can be detected is by using a supervised machine learning approach in which historical instances of suspicious activity (e.g., past Suspicious Activity Reports or risk relevant investigations) are used as training labels.

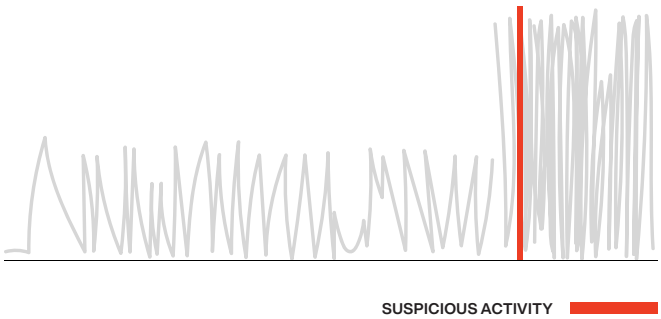


Figure 5: *Supervised machine learning approach used to classify suspicious activity*

In this approach, the supervised model learns the optimal interactions of complex time-based features to best classify suspicious activity for prioritized investigations.

An ensemble of decision trees, such as Gradient Boosted Decision Tree, is a common supervised modeling method that accurately detects suspicious activity while maintaining interpretability of the feature interactions and model output. In a tree-based model:

- Each node in the decision tree represents a complex machine learning feature.
- The model will permute every possible tree, threshold, and combinations of trees, to determine the optimal configurations.
- The machine learning features are ranked by importance in determining suspicious cases.

Simplified Example of One Tree

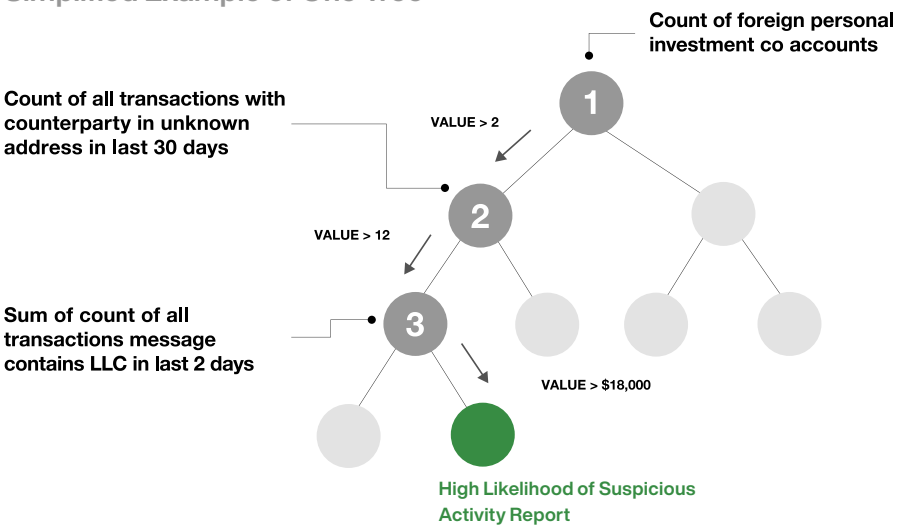


Figure 6: *Simplistic example of a decision tree*

4. Review Results and Tune the Model

After the machine learning model has been trained on an organization's dataset, the model is tested to assess its performance on a subset of previously unseen data (i.e., data not used for model training). The model performance is assessed and tuned by replaying history and analyzing the accuracy of model predictions during the historical period.

When analyzing a model that is trained to detect suspicious activity and prioritize case investigations, the model may be tuned to optimize two key drivers of value:

1. **Efficiency** – What is the reduction in false positive or unproductive alerts?
2. **Effectiveness** – How large is the increase in correctly identified suspicious activity?

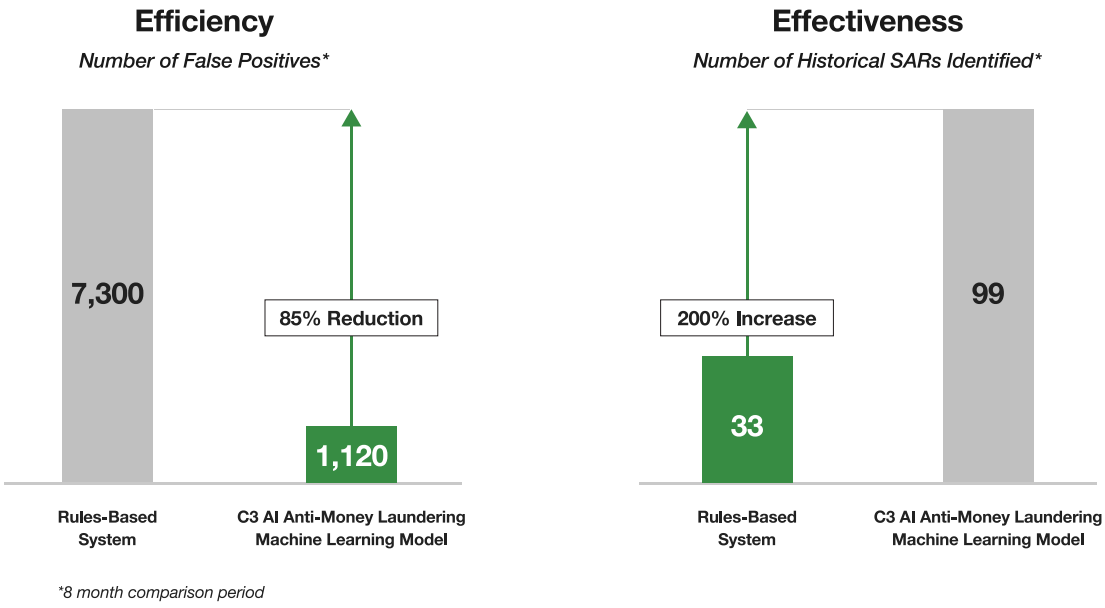


Figure 7: *This model is tuned to optimize key driver values: efficiency and effectiveness.*

5. Prepare Evidence Package

The model output should be prepared and presented in an interpretable way to support case reviews, audits and regulatory approvals. C3 AI AML's model evidence package helps AML investigators understand the reasons behind the AI-driven risk score, review the model outputs by familiar typologies, and deep-dive into the individual features and raw data that produced each risk score.

Typology	Feature	Contribution	Value
High-Risk Associations	Count of ALLINN related party transactions between 5,000 and 10,000 in last 180 days	0.249	1.0
Unusual Fund Transfer	Count of HIROUT transactions between 10,000 and 100,000 in last 180 days	0.192	23.0
Cross-Border Transactions	Sum of count of all transactions message contains panama in last 180 days	0.188	1.0
Lack of Transparency	Account holder added industry code in last 90 days	0.118	0.0
Tax Evasion	Sum of value of all transactions message contains tax in last 180 days	-0.108	0.0
Unusual Fund Transfer	Change in avg. count of ALLOUT transactions in last 180 days compared to previous 180 days	-0.102	0.174
Activity Inconsistency	Sum of value of all transactions message contains company in last 180 days	0.093	405,000
Unusual Fund Transfer	Count of ALLOUT transactions between 10,000 and 100,000 in last 180 days	-0.062	2.0
Unusual Fund Transfer	Stddev count of HIROUT transactions in last 180 days	0.051	0.083
Lack of Transparency	Sum of value of all transactions message contains LLC in last 180 days	0.011	0.0
Lack of Transparency	Count of all transactions with counterparty in different financial institution in last 2 days	-0.004	1.0

Table 2: *C3 AI AML's model evidence package helps AML investigators understand the reasons behind the AI-driven risk score, review the model outputs by familiar typologies, and deep-dive into the individual features and raw data that produced each risk score.*

6. Improve ML Model with Implementation

Finally, after the model is deployed and predictions are being used to prioritize AML investigations, a feedback loop is used to improve model performance over time. C3 AI AML's native workflow capabilities and application user interface provide a mechanism for investigators to provide feedback on the model output. As the model receives feedback on its predictions, it is retrained on improved labels augmented with user input.

05

C3 AI Anti-Money Laundering

Transforming Financial Crime Detection with Machine Learning

C3 AI Anti-Money Laundering

C3 AI® Anti-Money Laundering is an AI-enabled, workflow-centric application that uses comprehensive machine learning techniques to reduce false positive alerts by as much as 85%, while increasing true suspicious activity report (SAR) identification by as much as 200%. The application increases the efficiency and effectiveness of financial crime identification teams by providing intelligent and autonomous suspicious activity triage, issue resolution workflow, and automated evidence packages for regulatory reporting.

External Data
Relevant watch list and regulatory report data surfaced for the client

Analysis Tabs
Screens to deeply explore activity, associations, and time series data

Risk Score
Driven by comprehensive machine learning algorithms

Key Risk Drivers
Risk score is broken down into interpretable risk drivers

Key Metrics
Summary of key metrics for the client over time

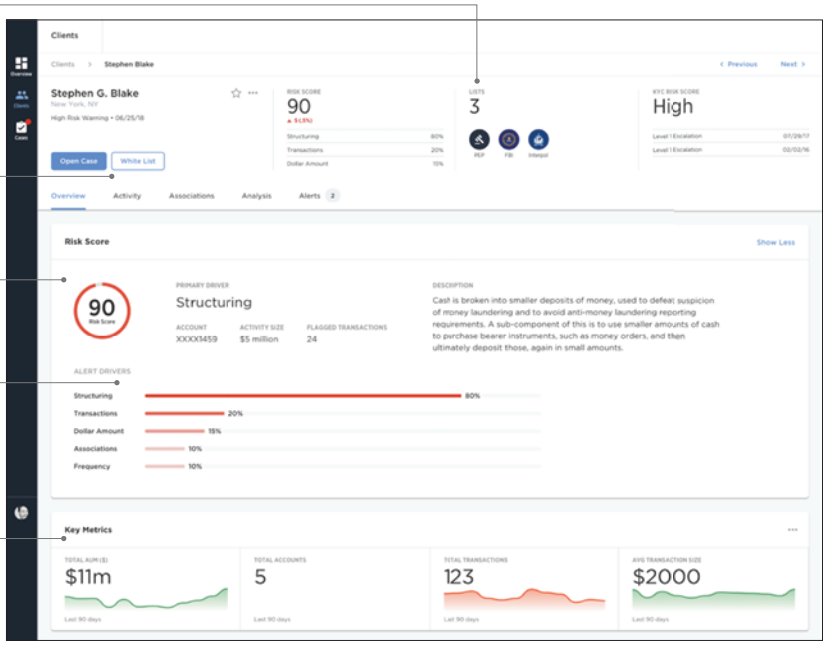


Figure 8: *C3 AI Anti-Money Laundering application.*

Figure 9: *C3 AI Anti-Money Laundering benefits.*

C3 AI Anti-Money Laundering delivers:

- **Improved Alert Quality:** Reduce false positive alerts and focus on highest risk cases.
- **Increased Team Productivity:** Integrated case investigation workflows, rich contextual visualizations, and case recommendations lead to greater investigation efficiency.
- **Accurate Risk Scoring:** Increase suspicious activity algorithm precision through continuous feedback from investigations.
- **Interpretable Machine Learning:** Empower investigators by explaining key risk drivers and creating an audit trail for reporting needs.
- **Unified Data Image:** Correlate data from internal and external data sources including transaction data, KYC system client information, adverse media, sanctions, PEP lists, and case management systems.
- **Flexible Data Integration:** Easily integrate C3 AI AML within your enterprise using RESTful APIs.
- **Intelligent Client Segmentation:** AI-driven behavior-based segmentation enables deeper understanding of clients.
- **Extensible and Configurable:** Detect emerging money laundering typologies and configure new analytics by scenario.
- **Near-Real-Time Updates:** Holistic client risk scores are updated with every transaction or account activity.
- **Robust Case Management:** Advanced tools enable escalation, collaboration, case auditing, and automated evidence package creation and SAR filing.

06

How It Works

Case Study: F50 Bank

Company

A large, multi-national bank operates AML compliance programs to identify and report money-laundering and other suspicious activities across its 15 million global customers.

Figure 9: *F50 Bank who operates AML compliance programs.*

Challenges

Growth in cross-border transactions, changing standards, heightened regulatory scrutiny, and the increasing complexity of money laundering strategies and tactics have made it difficult for the bank to efficiently scale its compliance systems to meet AML requirements. In particular, the bank faces a critical constraint familiar to many financial institutions: existing customer due diligence, transaction monitoring, and triaging solutions that utilize simplistic analytics and rules-based models that struggle to identify complex money laundering typologies.

Traditional-rules-based solutions often lack extensibility and thus cannot easily adapt to evolving risks. Further, these solutions cannot aggregate data siloed in disparate systems. In addition, the bank needed a solution that was proven and field-tested, met regulatory scrutiny, improved team productivity, and future-proofed them to new suspicious activity typologies. Seeking to reduce false positive alerts and investigate cases more efficiently, the bank selected C3 AI to deploy a holistic machine learning solution to dramatically improve the identification and triage of money laundering and other suspicious activity.

Solution

C3 AI and the bank worked together to integrate relevant data and apply scalable, production-ready machine learning algorithms to detect suspicious activity. Data from 11 sources were unified and federated into more than 40 logical C3 AI Models representing the timed nature of relationships between clients, accounts, transactions, countries, and counter-parties.

With a comprehensive data image in place, the raw data was automatically enriched to identify actionable, typology-driven signals associated with money laundering. Compared to traditional, rules-based solutions that use fewer than 300 rules, C3 AI Anti-Money Laundering offers more than 5,000 out-of-the-box time-based expressions that fully represent the richness of information in the underlying raw data. These expressions structured raw data, utilized natural language processing, and leveraged graph traversals to capture information relating to party and account characteristics, illicit networks and associations, transaction patterns and behaviors, and additional potential signals of money laundering and other suspicious activity. A sophisticated and interpretable machine learning algorithm was trained using these signals to detect multiple typologies of suspicious activity among clients. The algorithms delivered human-interpretable insights relating to the key risk drivers via an intuitive user interface. Further, the application produced evidence packages that are investigator and regulator-ready.

Results

Figure 10: *F50 Bank AML results*

View the C3 AI Anti-Money Laundering case study to learn more.

07

C3 AI + FIS: Reimagining Banking with AI

C3 AI is an enterprise AI technology leader and has partnered with FIS, a financial technology leader, to accelerate the digital transformation of the financial services industry. FIS™ AML Compliance Hub powered by C3 AI leverages C3 AI's advanced machine learning technology, combined with the deep financial industry domain expertise of FIS, to dramatically improve the efficiency of financial crime detection.

FIS AML Compliance Hub significantly improves investigator productivity with intelligent case recommendations, automated evidence packages, and advanced visualizations of key contextual case data, such as alerts, parties and counter-parties, accounts, transactions, and risk drivers. In addition to integrating traditional core banking and transaction monitoring data, the AML solution delivers a universal view of the customer by integrating data from internal know-your-customer systems and external sources such as adverse media search results, sanctions, and politically exposed person (PEP) lists. As a result of these and other advanced AI-enabled capabilities, FIS AML Compliance Hub powered by C3 AI minimizes false positive alerts and increases suspicious activity report (SAR) identification.

08

Ready to Get Started?

Learn how you can unify data from across the bank to improve the efficiency and accuracy of your AML operations.

Contact Sales

sales@c3.ai

Learn More & View Demo

https://c3.ai/products/c3-ai-anti-money-laundering/

Download Data Sheet

https://c3.ai/resources/data-sheet/c3-anti-money-laundering-data-sheet/