McKinsey & Company

Risk & Resilience Practice

The fight against money laundering: Machine learning is a game changer

To realize the full benefits of machine learning and advanced analytics in anti–money laundering, institutions need AML experts, strong data science talent, and reliable data sources in the fight against this type of financial crime.

This article is a collaborative effort by PK Doppalapudi, Pankaj Kumar, Adrian Murphy, Christophe Rougeaux, Rick Stearns, Scott Werner, and Shuo Zhang.

October 2022

The volume of money laundering and other financial crimes is growing worldwide—and the techniques used to evade their detection are becoming ever more sophisticated. This has elicited a vigorous response from banks, which, collectively, are investing billions each year to improve their defenses against financial crime (in 2020, institutions spent an estimated $214 billion on financial-crime compliance).[1] What's more, the resulting regulatory fines related to compliance are surging year over year as regulator's impose tougher penalties. But banks' traditional rule- and scenario-based approaches to fighting financial crimes has always seemed a step behind the bad guys, making the fight against money laundering an ongoing challenge for compliance, monitoring, and risk organizations.

Now, there is an opportunity for banks to get out in front. Recent enhancements in machine learning (ML) are helping banks to improve their anti-money-laundering (AML) programs significantly, including, and most immediately, the transaction monitoring element of these programs. Moreover, US regulators are strongly backing these efforts. Including the Anti-Money Laundering Act of 2020 and the subsequent National Illicit Finance Strategy, US agencies are reducing obstacles from existing regulations, guidance, and examination practices to encourage banks to test and adopt innovative approaches for fighting financial crimes.[2]

This momentum in the fight against financial crimes is creating keen interest in ML among industry leaders. Earlier this year, McKinsey invited the heads of anti–money laundering and financial crime from 14 major North American banks to discuss adopting ML solutions in transaction monitoring. More than 80 percent of the participants had begun the process of adopting ML solutions, with most expecting to dedicate serious efforts to implementing ML solutions within their AML programs in the next two to three years.

Applying machine learning to transaction monitoring

In theory, banks can apply ML across the entire AML value chain (Exhibit 1). But we believe that transaction monitoring—specifically, combining ML with other advanced algorithms (for example, random forest, gradient boosting, deep learning)—is where banks can reap one of the most immediate and significant benefits in their AML efforts.

Transaction monitoring—specifically, combining machine learning with other advanced algorithms—is where banks can reap one of the most immediate and significant benefits in their anti–money laundering efforts.

[1] *True cost of financial crime compliance study*, LexisNexis, 2020.
[2] See "Treasury announces 2022 National Illicit Finance Strategy," US Department of the Treasury press release, May 13, 2022; "Treasury's FinCEN and federal banking agencies issue joint statement encouraging innovative industry approaches to AML compliance," Financial Crimes Enforcement Network (FinCEN), US Department of the Treasury, December 3, 2018; and "FinCEN's Innovation Initiative," FinCEN, accessed September 27, 2022.

Exhibit 1

A spectrum of sophistication exists in analytical approaches throughout the anti-money-laundering value chain.

Analytical approaches, not exhaustive

	Existing	What is next
Client risk rating (CRR) on onboarding	• Expert weighted-factor approach • Traditional statistical-regression approach	• Use of advanced algorithms (statistical or machine learning [ML] approach)
Client screening	• Sanctions screening • Negative media screening	• Advanced algorithms (eg, multi-entry match) with feedback mechanism
Transaction monitoring (TM)	• Rules-based approach • ML as point of contact or on top of the existing rules-based engine	• Use of ML to improve effectiveness and efficiency • Expansion of data envelope across multiple data sources
Event-driven review	• Additional rules introduced through time on top of TM-system-scheduled know-your-customer (KYC) refreshes	• Dynamically introduce highly precise rules for newly identified risks • Option remains for intelligence-expert-driven rules
Transaction filtering and screening	• Sanctions screening using simple matching algorithms • Negative media screening	• Advanced algorithms with feedback mechanism
Refresh (CRR + expected vs actual)	• KYC calendar-driven approach • Comparison of actual vs expected transactions	• Perpetual KYC through behavioral scores • ML models to drive client segmentation and identification of anomalous behaviors

Today, many financial institutions use rule- and scenario-based tools or basic statistical approaches for transaction monitoring. These rules and thresholds are driven primarily by industry red flags, basic statistical indicators, and expert judgment. But the rules often fail to capture the latest trends in money-laundering behavior. Machine learning models, on the other hand, leverage more granular, behavior-indicative data to build sophisticated algorithms. They are also more flexible in quickly adjusting to new trends and continually improving over time. By replacing rule- and scenario-based tools with ML models, one leading financial institution improved suspicious activity identification by up to 40 percent and efficiency by up to 30 percent.

When transitioning to an ML model for transaction monitoring, banks should address three key questions:

Where should banks use machine learning?
For starters, it is important for banks to understand the circumstances where they can use ML effectively and where they can't. Machine learning is certainly advantageous when there is a high degree of freedom in choosing data attributes, as well as sufficient availability of quality data (for example, in scenarios where there is a rapid movement of funds and a large number of attributes can be considered). ML is also appropriate when it becomes difficult to identify the dynamics and relationships between risk factors.

However, ML is not useful when there is not enough existing data to build forward-looking

intelligence. In these cases, a traditional approach (rule- and scenario-based tools, for instance) could be more effective.

What additional data sources are needed?
When working with suspicious-activity reports, poor quality data inevitably leads to poor model performance. It is important, for example, not to be too dependent on suspicious-activity-report categories (for example, structuring, terrorist financing, money laundering, fraud), which are limited in today's world. With this in mind, institutions are exploring a range of initiatives to improve data gathering for their ML models to provide enriched context for transaction monitoring. This includes modeling against individual transactions or cases, components of suspicious-activity-report filings or client relationships terminated for AML reasons, and data from historical subpoenas and other law enforcement requests for information.

These more complex ML models can incorporate a wide range of new elements and variables, such as the following:

— *enhanced client data* (for example, nature of business, type of clients)

— *more comprehensive product data* (for instance, granular product type and usage)

— *more granular channel data* (for example, channels for different products)

— *risk indicators across risk type* (for instance, business geography)

— *external data sources* (for example, bureau data, financial-crime registries)

How should banks service the model?
ML models are less transparent than rule-based ones, and model risk management (MRM) teams and regulators are increasingly demanding better model "explainability"—that is, better methods of interpreting "black box" machine learning models, which develop and learn directly from the data with typically no human supervision or guidance—so they can assess the models.

At leading institutions, model development teams are working with AML investigators to help ensure that the teams understand the modeling data, create interpretable modeling features rather than a data dump, and integrate ML modules with existing rule- and scenario-based models and tools (that is, the transition process should leverage the existing platform, thus improving the status quo and not dismantling it entirely). Leading institutions are also starting to create AML-specific model guidelines. Some of the specific ways that banks are improving explainability and generating more high-quality alerts for downstream investigators include the following methods:

— *Out-of-time sample:* Banks must reserve sufficient testing samples to conduct model testing.

— *Model validation:* Banks consider ML-specific risks, including feature engineering, hyperparameter calibration, model bias against protected classes, model drift and interpretability, transparency, and explainability.

— *Ongoing monitoring:* Banks conduct frequent, ongoing, below-the-line (BTL) testing to help monitor model performance.

Best practices for bringing machine learning to transaction monitoring

We have identified three best practices that leading financial institutions can use to adopt ML for AML transaction monitoring:

1. Align stakeholders on vision and design
One of the primary reasons that ML projects fail is because of a lack of buy-in from various stakeholders, including the data, technology, line-of-business, MRM, and compliance teams. It is critical to engage these stakeholders from the beginning of the project to align on vision,

to make architectural design choices, and to consider trade-offs for all processes from end to end (Exhibit 2). This helps to ensure that all business-as-usual activities and ongoing regulatory actions are considered. For example, leading institutions will often start meeting with regulators up to a year before development even begins—and then through the development process—to avoid surprises.

Ultimately, gathering multiple perspectives and aligning on the vision, design, and trade-offs for using ML improves transparency across the enterprise while uncovering and reducing risks. The value proposition is tied to improving effectiveness by better capturing the risk and generating high-quality alerts for downstream investigation—efficiency, therefore, follows effectiveness.

2. Develop a safe technology transition plan

Transformations are about more than just adding new technologies. For successful transformation, we believe three key elements matter most:

— *Be intentional about the approach* (for example, focus on the transition plan, not just the end state).

— *Adopt a collaborative mindset that fuses technology and business goals* (for instance, for the user, by the user—involve the business at all times and in all phases of the process).

— *Proceed with rigorous and transparent execution tailored to the realities of modern technology systems* (for example, apply a modular approach to plug and play).

Exhibit 2

Banks need to consider several design choices when developing anti-money-laundering approaches for transaction monitoring.

Dimensions for consideration, not exhaustive

Data

Intended application
- Suppress and/or prioritize scenario outputs
- Input to individual and/or multiple scenarios
- Replace individual scenario and/or multiple scenarios

Enriched data (aside from current transaction-monitoring data)
- Customer/product/channel
- Counterparty
- Risk (eg, fraud, cyber, sanctions, negative media)
- External (eg, personal, corporate identification)

Targeted variable
- PVA, SAR[1]
- Scenario vs client level
- Period for which customers are interesting[2]
- Treatment for linked accounts

Methodology

Interval of analysis
- Daily
- Weekly
- Monthly
- Quarterly

Sampling
- Definition of known population
- Stratified sampling for unknown population
- Development vs out of trend
- Adjustment for historical data

Algorithm (deep dives follow)
- Feature engineering
- Machine learning algorithm
- Test metrics (precision, recall)

Monitoring and implementation

Monitoring
- Metrics and thresholds
- Governance and decision support

Implementation
- Data storage
- Model calculation
- Alert production
- Case management

[1]Population variability analysis, suspicious activity report.
[2]Time period in which there was a high volume of customers or accounts that would be of interest to the model.

However, all technology transformations experience setbacks. Employees often resist adopting new ways of working, and new technologies can introduce unforeseen risks. To win early support during the pilot phase and to help minimize risks, a bank could run existing rule- and scenario-based risk scenarios in parallel with ML-based scenarios to build confidence among stakeholders.

To further encourage adoption and reduce risk, the company might choose projects that can leverage existing platforms (those that employees are already comfortable using) and integrate the new components one at a time. Ideally, banks will start with the low-hanging fruit—projects that offer significant potential rewards with manageable risk.

3. Enhance the model risk management framework

To incorporate ML solutions into the transaction monitoring framework, MRM teams need to do the following:

- *Expand capabilities* to work closely with the data science team in the model development and validation process. MRM teams should educate data scientists about potential risks during the development process and have the analytics know-how to participate in the validation process.
- *Shape validation standards, policies, and frameworks* to address the specific risks associated with ML models, including bias detection and explainability.
- *Define precise performance and monitoring requirements,* including BTL, out-of-time testing, and when to recalibrate ML models. MRM teams should automate these performance and monitoring tests.

Machine learning is the future for anti–money laundering

In the fight against money laundering, banks have traditionally been one step behind the bad guys. Now, banks have a chance to change the game. Advanced-analytics techniques, particularly machine learning with network analytics, promise to improve transaction monitoring dramatically by reducing false-negative and false-positive rates—and by sending higher-quality alerts to downstream anti-money-laundering investigators.[3] For most banks, the development requires investing significant time and resources. To realize the full benefit, institutions will need to build a talent pool, create reliable data sources, and leverage the knowledge of subject matter experts. A tall order, but well worth the effort given the stakes.

PK Doppalapudi is a consultant in McKinsey's Charlotte office; **Pankaj Kumar** and **Adrian Murphy** are partners in the New York office, where **Scott Werner** is a senior expert and associate partner and **Shuo Zhang** is a consultant; **Christophe Rougeaux** is an associate partner in the Waltham, Massachusetts, office; and **Rick Stearns** is a senior adviser in the Washington, DC, office.

Designed by McKinsey Global Publishing

[3] *Banking & Securities matters*, "Network analytics and the fight against money laundering," blog entry by Daniel Mikkelsen, Bryan Richardson, and Dan Williams, McKinsey, August 15, 2019.