WHITE PAPER

Next-generation AML

6 tips to modernize your fight against money laundering

Contents

Rapid digitization spurred by faster payments and the pandemic increased financial crimes to unheard-of levels over the past few years. Those who fight money laundering now face more complexity, additional types of risks, more suspicious activities and tighter regulatory requirements. But most firms are still working with the same resources. Doing more with less – and doing it faster and better – is a top priority for financial institutions.

That's where next-generation anti-money laundering (AML) comes into play.

Next-gen AML involves using leading-edge technologies like AI and machine learning (ML) to make AML programs more efficient and effective. Such technologies automate manual processes such as data consumption and analysis, resulting in faster, earlier event detection and scoring. Techniques like natural language processing manage unstructured data and automatically generate suspicious activity report narratives. Advanced analytics streamlines the decision-making process by triaging alerts and determining which do – or do not need to be acted on immediately.

Today, most firms are taking a hybrid approach with their AML programs – using existing processes in conjunction with next-gen AML capabilities. Over time, this will shift as more firms incorporate next-gen AML capabilities into their routine operations.

Next-gen AML helps financial institutions take a modern approach to fighting financial crimes by reducing risk and improving overall operational efficiency. This approach uncovers more cases of money laundering. It also reduces time spent chasing false positives, enables financial institutions to make better use of limited resources and helps them meet regulatory requirements with transparency.

Let's review six tips to help you succeed as you shift to next-gen AML.

The drawbacks of rules:

- Their view is too narrow.
- They take a hindsight approach.
- They're unwieldy to maintain.

1. Evolve beyond rules with a hybrid approach

The traditional way of monitoring transactions with rules-based systems is insufficient for meeting today's fast-paced financial crime landscape and ever-evolving AML compliance and counter-financing of terrorism (CFT) regulatory obligations. Rules-based systems:

- **Have a view that's too narrow.** Perfectly normal behavior for one entity might indicate money laundering activity for another. While firms can deploy behavioral monitoring by segmenting similar entities, there are often too few features to be effective.
- **Take a hindsight approach.** Such a view is based only on what you know about past patterns. For example, a rule might state that a certain transaction frequency, dollar amount or beneficiary is associated with legitimate transactions for an entity – while more nuanced and emerging interactions go unnoticed.
- **Are unwieldy to maintain.** Rules are relatively easy to circumvent, yet they're hard to maintain. The moment threats evolve, the rules need to be modified to reflect new risk exposures. Manual, rules-based processes struggle to keep pace with digital banking risks.

AI and ML can help you overcome these limitations. But few firms are ready to abandon their rules-based systems and fully replace them with analytical models and robotics. A hybrid approach is the answer.

Rules versus models

With a hybrid approach, you continue to use rules where they can do the job and use models where rules would fall short. For example, you may not need a model if patterns are precisely defined. Or perhaps the target areas or the outcomes are so rare that it would be too difficult to automate fully.

Analytical models shine in situations that call for discerning complex patterns from well-defined behaviors. For instance, alert scoring and hibernation models can clarify the risk associated with a package of alerts rather than just looking at a single transaction. This approach helps you get more value from your traditional transaction monitoring system.

Advanced analytics techniques can also identify common and expected patterns to track anomalies or false negatives – potentially suspicious activities that rules-based detection engines might miss. For example, one wire transaction alone may not look risky, but when you see it combined with additional activities, it could raise suspicion. Financial institutions are moving away from looking at individual activities and are looking more holistically toward an entity's behavioral profile or multiple activities that can drive a successful case.

Analytical models shine in situations that call for discerning complex patterns from well-defined behaviors.

2. Take a hard look at your data foundation and legacy systems

Improving data quality is key to building a robust AML program. Yet data issues present a significant obstacle for many financial institutions. Internal data tends to be fragmented and incomplete and often resides in multiple disparate systems. Large banks' mergers and acquisitions create even more siloed systems and databases that feed into a compliance data hub. But they're not all connected.

To elevate defenses against financial crimes, financial institutions must address internal data inadequacies while enriching and integrating both internal and external data. This approach provides a holistic view of customers and enhances customer risk profiling. Financial institutions must invest in capabilities that ingest, integrate, link and manage numerous internal and third-party data sources to build a holistic customer profile and correctly translate that data into intelligent insights.

To elevate defenses against financial crimes, financial institutions must address internal data inadequacies while enriching and integrating internal and external data.

Data quality and governance

Data quality from SAS standardizes, deduplicates and corrects data to ensure clean, accurate data for analytics. Data governance tools allow you to set and enforce overarching rules that control how your organization collects, manages and archives data. This helps you to quickly and easily import all types of data, prepare it for analytics and resolve entities.

Data orchestration

Seamlessly aggregate and cleanse internal and external data from all relevant sources with a single, integrated data analytics platform. Then rapidly transform and enrich multiple data types – including transaction data, nonmonetary event data, geographic data, risk lists, third-party data and a variety of customer information – to use in monitoring.

3. Explore ML and AI techniques

It may be tempting to add more people to tackle the issues stemming from compliance pressures and increasingly sophisticated threats. But this is not a feasible approach for the long term. A better plan entails testing innovative techniques that can streamline processes and drive faster, more informed decision making.

Why not experiment with the latest technology, such as AI and ML, to see what advantages you can achieve? These techniques could help your financial institution significantly expand coverage of multiple risks while boosting the efficiency of your overall AML program.

With AI and ML techniques, you can:

- **Intelligently triage alerts.** Auto-referral or hibernation functions tap into a broad range of relevant information to expedite or hold off on escalating an alert for review.
- **Automate data collection for investigations.** ML can automate internal and external information gathering, like database queries and information collection from third-party data providers. This frees analysts and investigators to make crucial decisions rather than performing mundane, time-consuming tasks.
- **Generate notes and narratives automatically.** Natural language generation can auto-populate reports and expedite the production of case files and notes, creating efficiency and consistency.
- **Create a virtual digital assistant to streamline processes.** AI bots can determine how you usually navigate a system and suggest the next steps for your workflow.

Recognize and scan document types

At a tier-one bank, SAS deployed a combination of text mining, image recognition and ensemble models that processed **9 million** transactions, scanned **25 million** documents, automated **200** risk typologies and improved operational efficiency by **25%**.

AI techniques and their benefits for AML/CFT systems

Link analysis (also known as social network analysis) reveals complex networks of individuals, entities and jurisdictions and defines the nature and strength of possible collusion.

Correlation and regression analyses clarify the extent of dependence among multiple variables, which helps identify the attributes most predictive of criminal activity.

Cluster analysis uses unsupervised learning to classify entities into groups and subgroups with commonalities. This classification technique identifies behavioral anomalies that could indicate criminal activities.

Neural networks and predictive analytics tools analyze vast data sets to find hidden patterns and trends and model expected behavior to accurately spot false positives.

Natural language generation scans, extracts and classifies content from text and image sources to bring unstructured data into the detection process and streamline report generation.

Robotic process automation automates routine tasks, such as retrieving information to enrich alerts, reconciling data across systems and responding to common requests.

4. Continuously learn and improve with AI and ML

Financial crime threats evolve constantly. Broad criminal strategies change. The bad actors modify their methods to slip in undetected.

In today's financial crime threat landscape, financial institutions need more than just rules and standard analytics. They need smarter and more nimble surveillance. Using the latest innovations like AI and ML can effectively uncover new schemes or detect increasingly sophisticated financial crime schemes.

Whenever something new happens, you should account for it in new equations – which calls for continuous learning. For instance, if you've identified a new risk or built a new monitoring capability into your program, it may affect other areas you didn't realize would be affected. It may even affect investigators' priorities and workflow. AI can help you automatically deal with these new threats coming through the system.

ML can analyze historical outcomes and automatically adjust thresholds to reduce false positives. Lessons learned should be fed back to the system frequently for continuous improvement.

Before using AI to optimize detection, investigation and reporting, your AI solution must incorporate learnings from resolved case decisions. When you combine human investigators' expertise with AI, the system can effectively make recommendations and enhance the overall effectiveness of AML programs – while containing costs and helping to ensure compliance with regulations.

ML can analyze historical outcomes and automatically adjust thresholds to reduce false positives. Lessons learned should be fed back to the system frequently for continuous improvement.

Get more granular and rigorous

It's essential to take a more rigorous approach than simply dividing personal and commercial clients. That's a start – but once you've done that basic segmentation, you'll need to get more granular to reflect your business model. You could follow a basic approach, such as taking standard deviations and bucketing organizations into small, medium and large based on their total transactions. Or you could create segments by product or transaction type.

On the other hand, you could take a more sophisticated approach. For example, K-means clustering is a popular, unsupervised ML algorithm that makes inferences from the data based on input variables without referring to known outcomes. This analytical technique helps you understand how variables interact and naturally clusters entities into different groups. Once you've accomplished that, you can zoom in on your scenarios and look closely at risks specific to those clusters.

Hibernation and alert generation

Auto-referral or hibernation functions tap into a broad range of relevant information to expedite or hold off on escalating an alert for review. By prioritizing high-risk alerts, parties and events, alert risk scoring ensures that you allocate resources to the most pressing activities.

5. Establish rigorous model governance

A comprehensive AML program establishes three lines of defense. First, you must quantify the risk and determine what you need to monitor. Second, develop controls. And third, make sure you're positioned to challenge those controls. You'll need to answer questions like:

- Are my algorithms still working?
- Are cases appropriately expedited or hibernated?
- Are models being monitored and tuned as necessary?

When it comes to model risk governance, it's better to be proactive than reactive.

To apply the necessary rigor around ML, you must evaluate, monitor and govern your AI techniques with appropriate oversight and controls. Such controls continually test and validate the process on the back end, which is essential for this type of program to work.

It's essential to tune and test your models as things change. Otherwise, they may become less effective over time. There could have been changes in the customer base that you need to account for. Or feedback from investigators may show that some scenarios need to be fine-tuned. By continually validating and challenging your models, you can ensure they remain the best for your business process.

Provide oversight for AI and analytical outcomes throughout the anti-financial crime process.

DEPLOY INSIGHTS

Test

Ensure models will perform as expected in the real world.

Deploy

Embed models into operational systems and monitor them. Integrate business rules to ensure up-to-real-time results.

Govern

Make sure decisions are safe and transparent over the life of the model.

Visualize & Report

Understand more with embedded explanations of data and models in simple language.

Deploy complex analytics projects into production and keep them there. SAS can help you automate tasks, govern decisions and deploy every type of model quickly.

You can test and determine the best-performing (champion) model through multiple iterations using several different techniques and document everything as you go. These steps are invaluable as you delegate more operational processes to machines. You'll always need to monitor how those machines are making decisions. Model monitoring – and transparency in general – take on new emphasis, considering the relative lack of transparency in some autonomous, self-learning approaches.

By having the proper controls in place, you'll be able to show regulators, examiners and your internal audit teams the evidence of how you arrived at a decision. Your controls will demonstrate that you're following a standard model validation process and documenting testing and changes along the model's entire life cycle. By showing how you arrived at a result, you can support your decision and prove that the results can be replicated.

6. Be prepared to adapt

As you shift into next-gen AML, it's essential to keep reevaluating your approach so that you can adapt as times change. Consider these key points when thinking about the future:

- **The cloud.** Firms have already started to move to the cloud. It's easier to keep pace with technology changes in a cloud-based environment. It's also more economically feasible and is highly scalable, resilient and sustainable. AML operations will eventually move to the cloud as well. Keep the "cloud future" in mind as you adopt new systems and processes.
- **The role of analytics.** Everyone should be empowered to use analytics to make faster, better decisions. By taking advantage of advancements in computing capabilities, automation, advanced analytics and cloud-based technology, you can strengthen regulatory compliance while taking a risk-based approach to fighting financial crimes.
- **Ease of use.** Adopt analytics that is easy to use. And invest in your people, keeping in mind that:
  - Humans will still need to do the heavy lifting and the high-value work in the future.
  - Machines will do the lower-value, repetitive work.

Embarking on a path to modernization can be complicated – requiring time, resources and funding. But today's technological advancements give financial institutions the tools they need to modernize AML compliance frameworks – it pays to be prepared.

On your journey to adopting new financial crime technologies, be sure to define your organization's unique objectives. And prioritize technology adoption based on its importance to the effectiveness of your financial crime ecosystem.

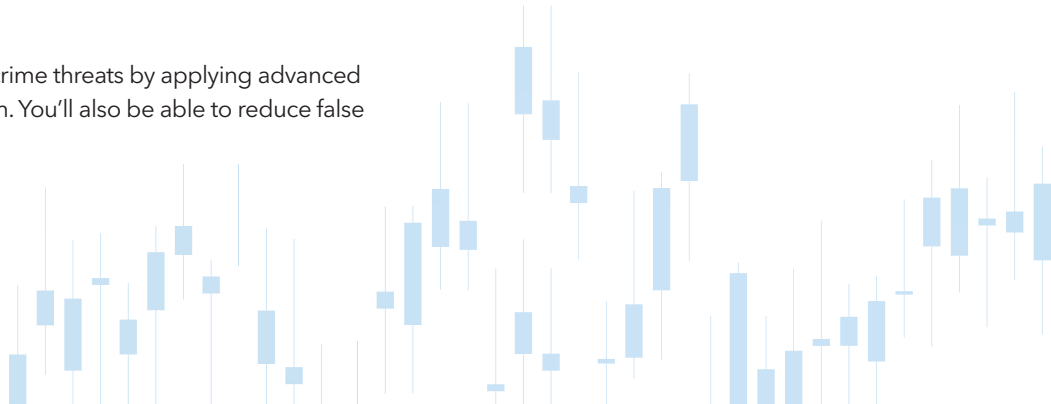
Next-gen AML from SAS

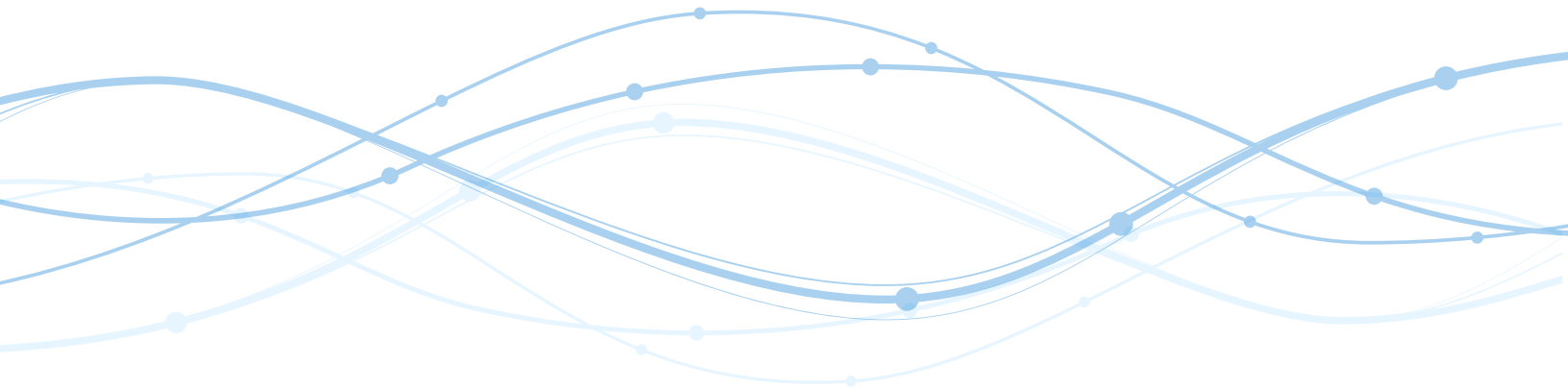
As the financial services industry undergoes massive digital transformation and regulators keep upping their definition of "reasonable" control and governance, next-gen AML will continue to be central to the evolution.

Instead of simply reacting to past information, rely on ML and AI to achieve a forward-looking advantage. You can distill new data elements not previously known or available for AML models. Let the computer uncover patterns the human eye would never see. Validate those insights and feed the results back into your models. The more training a model gets with feedback data, the smarter it becomes.

Leading-edge analytics and hybrid modeling techniques detect AML and CFT threats faster and more accurately than traditional methods. Embedded ML enhances every step of the process – continuously fine-tuning detection algorithms, streamlining and automating investigative and reporting processes, and boosting overall efficiency while reducing cost.

Your organization can uncover more financial crime threats by applying advanced analytics and powerful ML on a unified platform. You'll also be able to reduce false positives and run more efficient investigations.





Learn more about next-gen AML from SAS.