



## 4 Ways AI Can Boost Your AML Programs

**Artificial intelligence helps fight money laundering by finding previously hidden, potential risks and enabling a reduced number of false positive alerts that the AML teams need to investigate.**



With the escalating technological sophistication of financial criminals, institutions are harnessing advances in artificial intelligence (AI) and machine learning to boost the effectiveness of their anti-money laundering (AML) programs. AI can be used to increase the accuracy of risk assessments, help uncover hidden networks, and enable faster identification of red flags and patterns indicative of illicit financial transactions.

With that in mind, let's explore four ways that AI can be applied to step up the fight against financial crime.



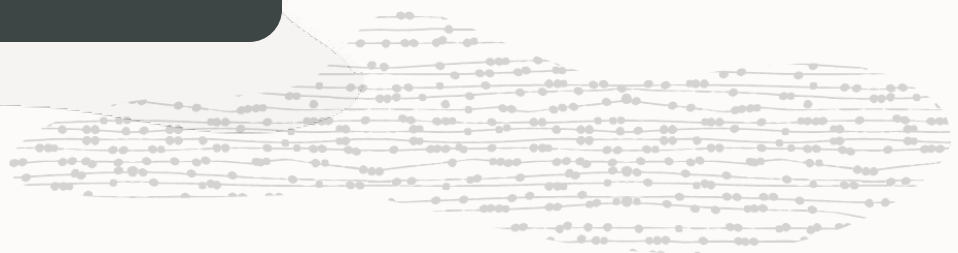
# 1. Enhancing customer profiles

Accuracy stems from the integrity and the availability of your data. Traditional know-your-customer (KYC) models are limited to looking at profile-only information provided by customers, which often are referred to as “static data.” With AI KYC models, machine learning broadens the possibility to include behavioral data such as how customers are interacting with a product or service, including their actions and events. These additional insights could better inform and determine the risk score associated with the customer profile to detect risky behavior faster and more efficiently.

“Integrating AI into AML compliance processes delivers enhanced decision making, more focused investigations and the ability to interpret large amounts of data with the right context, which helps financial institutions better manage their resources while meeting both their customer and regulatory expectations.”

**Jason Wynne**  
SVP Finance at Oracle  
Risk and Compliance Product Development

Integrating AI into AML compliance methods allows faster processing, analysis of enormous amounts of data, and improvements in handling complex tasks, which helps financial organizations better manage their resources. Replacing more traditional rules-based software tools with AI-based AML applications improves financial institutions' ability to identify suspicious activities by up to 40%, McKinsey & Company reports.





## 2. Eliminating noise

Rules-based scenarios cast a wide net that results in false positives. When criteria are too broad, the rules become less effective. When criteria are too narrowly set, the rules may let bad actors slip by. Instead of relying on and limiting to the traditional approach, behavioral models that are designed to identify possible criminal behaviors can take its place. This enables the dual effect of providing better risk coverage and reducing false positives.

“It’s not just an effective transaction monitoring system on its own or an effective KYC risk model that gives you broad protection against criminals. Instead, it’s the interaction of all the different controls and systems together that give you the best opportunity to catch criminals.”

**Jason Somrak**

Chief of Product and Strategy at Oracle  
Financial Crime and Compliance



### 3. Enhancing rules when they still must be run

Supervised machine learning can replace rules with surgical behavioral models, but it can also be used to make rules more effective. Traditional scenarios are rules-based where binary decisions determine if a transaction or activity is good or bad. While firms spend lots of time decisioning the noise created by rules, the labels generated in those decisions can be used to train models that improve the scenario performance. These labels can be an overlay on top of rules-based systems to allow improved output by generating a prediction score on new alerts that is based off prior decisions. As such, the prediction score could help determine if the new alert has a similar risk composure as those previously identified.



## 4. Enabling reduced compliance costs

The volume and cost for institutions to maintain their detection and investigation arms hinders their ability to quickly transform and adapt processes. As firms grow, so do their transaction volumes and a byproduct of that is more alerts and cases, which could mean more investigators. Generative AI can help control these costs by allowing firms to deploy agentic investigators that are designed to investigate hypothesis, build case evidence, query systems and draft a final narrative. This new frontier of AI holds great promise to bring greater reliability in decision making while helping to reduce costs.

“AI models can help call out shell companies, individuals, bank accounts, or entities even though they may appear unrelated in individual transactions.”

**Jason Somrak**

Chief of Product and Strategy at Oracle  
Financial Crime and Compliance





# Incorporating AI into AML

AI continues to demonstrate its ability to empower financial institutions to combat the increasingly sophisticated and complex nature of money laundering.

But many AML processes still run on legacy IT systems. To take advantage of AI, institutions should consider making the investment to build connectors with older transaction monitoring and reporting systems and modernize their infrastructure to handle the demands of AI. They also want to examine their objectives by implementing AI with clearly defined success criteria such as lowering operating costs, maintaining compliance, and countering money laundering.

As institutions consider adopting AI to help combat money laundering, they also should consider monitoring continuously evolving laws and regulations regarding AI to address compliance. Awareness of compliance obligations are key parts to building an effective, sustained AML program.

Prepare your anti-money laundering compliance program to discover emerging risks and criminal activity. Ready to incorporate AI into your anti-money laundering strategies to proactively combat financial crime?  
[Start here](#)

## Connect with us

Call +1.800.ORACLE1 or visit [oracle.com](https://oracle.com)

Outside North America, find your local office at [oracle.com/contact](https://oracle.com/contact)

Copyright © 2025 Oracle and/or its affiliates. This document is provided for information purposes only, and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document, and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.