

Oracle Financial Crime and Compliance Management Transaction Monitoring Cloud Service

Detect suspicious activity across traditional, real-time, and emerging payment channels with explainable, governed AML intelligence

Managing Financial crime is moving faster across payment channels, geographies, and customer relationships. AML teams must monitor higher volumes of activity, respond to new typologies, and meet reporting expectations without increasing operational burden.

Legacy monitoring approaches often rely on siloed data, static thresholds, and manual review cycles. The result is too many false positives, limited visibility into connected risk, and slower investigation decisions.

Oracle Financial Services Crime and Compliance Transaction Monitoring helps institutions unify transactional, customer, counterparty, and behavioral signals to detect suspicious activity, prioritize risk, and support explainable AML investigations at enterprise scale

Modernize AML transaction monitoring across channels and typologies

Oracle FCCM Transaction Monitoring is designed to help financial institutions detect and manage money-laundering risk with configurable rules, behavioral analytics, graph intelligence, adaptive scoring, and integrated investigations.

1. Ingest and normalize risk data: Bring together transactional, customer, counterparty, channel, device, and external risk signals through governed data integration patterns across real-time and batch sources.
2. Detect suspicious behavior: Monitor activity across payment rails using configurable scenarios, segmentation, AI/ML scoring, graph analytics, and what-if calibration to respond to changing typologies without bespoke code.
3. Investigate and report: Route high-risk alerts to the right teams, accelerate investigations with AI-assisted summaries and entity

Industry Challenges

- Rapidly evolving AML typologies across real-time, P2P, cross-border, scam, and emerging payment channels.
- High false-positive volumes that strain analyst capacity and slow investigation cycles.
- Siloed data across customer, account, counterparty, transaction, device, and external-risk sources.
- Pressure to tune scenarios, demonstrate model effectiveness, and meet jurisdictional reporting expectations.
- Need for explainable AI, human oversight, and regulator-grade auditability.

Transaction Monitoring Differentiators

- Comprehensive Coverage across 8+ current and emerging payment rails.
- Configurable rules, segmentation, and typology expansion without bespoke code.
- Behavioral analytics, graph intelligence, and explainable AI/ML risk scoring.
- Governed rule and model lifecycle with approvals, versioning, rollback, lineage, and monitoring.
- Integrated alert routing, case management, and AI-assisted investigations.

intelligence, and support audit-ready operational and regulatory reporting. Role-based user experience provides the right data at the right time for each user of the system from Chief AML Officers preparing for a board meeting to supervisors understanding and evaluating team performance.

Powered by Oracle FCCM workflows, analytics, and governed AI, transaction monitoring teams can move from reactive alert handling to risk-based financial-crime operations. Oracle brings rules, models, entity intelligence, queues, investigations, and reporting into a shared operating model.

With centralized monitoring and explainable risk scoring, institutions can improve coverage, reduce noise, and give analysts the context they need to make faster, defensible AML decisions.

Clarity in action translates to success

- Detect suspicious activity across wires, ACH, SWIFT, correspondent banking, real-time payments, P2P, wallets, disputes, scams, and emerging payment types.
- Improve alert precision with behavioral analytics, peer-group analysis, graph models, entity risk scoring, and adaptive scenario calibration.
- Use what-if calibration, ATL/BTL analysis, ROC curves, lift analysis, and alert-volume forecasting to improve scenario effectiveness.
- Route alerts based on risk, typology, skill, workload, jurisdiction, and SLA priority while preserving human oversight and audit trails.
- Accelerate investigations with AI Investigator summaries, suspicious-pattern identification, entity correlation, and explainable SAR narrative drafts.

By implementing Oracle FCCM Transaction Monitoring, financial institutions can help avoid costly operational and compliance outcomes:

- Reduce blind spots created by disconnected monitoring systems, fragmented data, and static rules.
- Prevent resource waste on ineffective scenarios, redundant controls, and manual threshold tuning.
- Support defensible decision-making with explainability, model guardrails, lifecycle governance, and reporting controls.

About Oracle Financial Crime and Compliance Management

Oracle Financial Services Financial Crime and Compliance Management (FCCM) is a comprehensive solution suite designed to address the demanding compliance needs of financial institutions. It covers transaction monitoring for AML and fraud, Know Your Customer, sanctions, transaction filtering and customer screening, enterprise case management, and regulatory reporting across different jurisdictions.

The suite incorporates advanced technologies including machine learning, graph analytics, natural language processing, and governed AI to enhance multi-dimensional risk scoring, money-laundering detection, and investigations with a pragmatic lens of enterprise adoption and scale. With more than 25 years of experience providing crime and compliance management technology solutions to more than 180 global financial institutions, Oracle FCCM helps institutions combat financial crime while supporting operational efficiency and regulatory oversight.

Key Features

- Interactive Rules-based scenarios with thresholds, segmentation, approvals, rollback, and effective-date controls.
- AI/ML scoring using anomaly detection, graph-based models, predictive analytics, and investigator feedback loops.
- What-if calibration with ATL/BTL analysis, ROC curves, lift analysis, and false-positive analytics.
- Intelligent alert routing using FIFO, LIFO, round-robin, SLA priority, skill-based assignment, and supervised override.
- AI Investigator for AML investigation summaries, escalation rationale, entity correlation, and SAR narrative drafts.

Key Benefits

- Demonstrable reduction in false positives while still detecting net-new risks.
- Approximately 80% reduction in manual rule tuning effort through automated calibration workflows.
- Regulatory-ready typology expansion through configurable logic and governed model updates.
- Proactive investigations can be initiated without waiting for an alert.
- Strict AML and fraud duty separation with role, jurisdiction, workflow, and data-access controls.

Connect with us

Call +1.800.ORACLE1 or visit **oracle.com**. Outside North America, find your local office at: **oracle.com/contact**.

 blogs.oracle.com/financialservices  linkedin.com/showcase/oraclefs  twitter.com/oraclefs  oracle.com/aml

Copyright © 2026, Oracle and/or its affiliates. All rights reserved. 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.

This device has not been authorized as required by the rules of the Federal Communications Commission. This device is not, and may not be, offered for sale or lease, or sold or leased, until authorization is obtained.

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

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group. 0521