Vendor Analysis

Vendor Analysis: Oracle

AML and Watchlist Monitoring Solutions, 2019

Chartis
Independent. Insightful. Actionable.

About Chartis

Chartis Research is the leading provider of research and analysis on the global market for risk technology. It is part of Infopro Digital, which owns market-leading brands such as Risk and WatersTechnology. Chartis' goal is to support enterprises as they drive business performance through improved risk management, corporate governance and compliance, and to help clients make informed technology and business decisions by providing in-depth analysis and actionable advice on virtually all aspects of risk technology. Areas of expertise include:

- Credit risk.
- Operational risk and governance, risk and compliance (GRC).
- Market risk.
- Asset and liability management (ALM) and liquidity risk.
- Energy and commodity trading risk.
- Financial crime including trader surveillance, anti-fraud and anti-money laundering.
- Cyber risk management.
- Insurance risk.
- Regulatory requirements including Basel 2 and 3, Dodd-Frank, MiFID II and Solvency II.

Chartis is solely focused on risk and compliance technology, which gives it a significant advantage over generic market analysts.

The firm has brought together a leading team of analysts and advisors from the risk management and financial services industries. This team has hands-on experience of implementing and developing risk management systems and programs for Fortune 500 companies and leading consulting houses.

Visit **www.chartis-research.com** for more information.

Join our global online community at **www.risktech-forum.com**.

© Copyright Infopro Digital Services Limited 2019. All Rights Reserved.

No part of this publication may be reproduced, adapted, stored in a retrieval system or transmitted in any form by any means, electronic, mechanical, photocopying, recording or otherwise, without the prior permission of Infopro Digital Services Limited trading as Chartis Research ('Chartis').

The facts of this document are believed to be correct at the time of publication but cannot be guaranteed. Please note that the findings, conclusions and recommendations that Chartis delivers will be based on information gathered in good faith, whose accuracy we cannot guarantee. Chartis accepts no liability whatever for actions taken based on any information that may subsequently prove to be incorrect or errors in our analysis. See **'Terms and conditions'**.

RiskTech100®, RiskTech Quadrant® and FinTech Quadrant™ are Registered Trade Marks of Infopro Digital Services Limited.

Unauthorized use of Chartis' name and trademarks is strictly prohibited and subject to legal penalties.

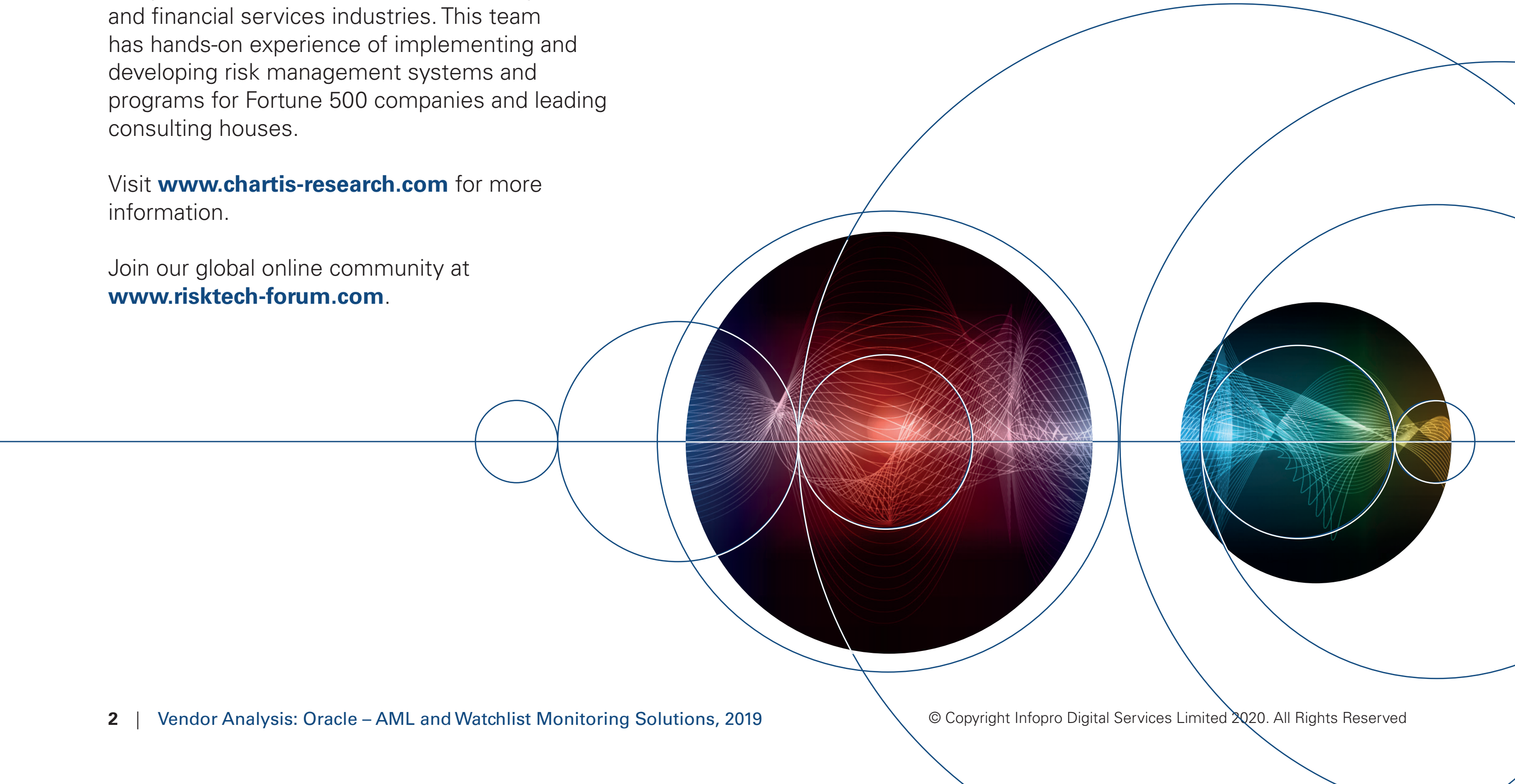


Table of contents

© Copyright Infopro Digital Services Limited 2020. All Rights Reserved

List of figures and tables

© Copyright Infopro Digital Services Limited 2020. All Rights Reserved

1. Report context

This Vendor Analysis is based on the Chartis quadrant report *Financial Crime Risk Management Systems: AML and Watchlist Monitoring; Market Update and Vendor Landscape, 2019* (published in March 2019). This section summarizes the key theses in that report; subsequent sections take a detailed look at Oracle's quadrant positioning and scoring, and Chartis' underlying opinion and analysis.

Key thesis

Market update

The anti-money laundering (AML) market landscape varies in its maturity and depth – while AML is well-established in western banks, for example, it is less mature in other geographies and industries. Within financial institutions (FIs), AML capabilities increasingly function on a continuum: centralized within specific compliance departments, but also present in other operational areas such as Know Your Customer (KYC) and customer lifecycle management (CLM).

In areas like retail banking where AML is relatively mature, FIs have reached an equilibrium. They are onboarding fewer suspicious customers, and growth in suspicious activity reports (SARs) – the primary AML indicator – has flattened. But these developments have come at the cost of large and hugely inefficient compliance departments, often containing thousands of employees.

FIs now want to reconfigure their existing AML processes to make them more efficient and valuable. But there has also been a shift toward understanding and quantifying AML solutions, rather than creating ever more complex tools and systems. This has sharpened the focus on model risk management and validation capabilities, to enable FIs to interrogate and authenticate existing models. Vendors and FIs are also considering new ways to express AML information, such as delivering it as a single headline figure (a 'compliance score' similar to a credit score).

As AML use matures in investment and retail banking, it is spreading into other areas, notably trade finance, gambling and the FinTech sector. Trade finance is an especially complex area for AML, with many constraints and a reliance on sometimes limited data that can vary across geographies. Nevertheless, trade-based AML is having a significant business impact on FIs, and is a valuable potential market for new vendors.

Vendor landscape

Packaged solution vendors and data providers remain the backbone of the AML marketplace. But new entrants, such as commercial workflow and advanced analytics vendors, pose a threat, especially to packaged solution vendors. FIs, especially large and complex ones, are looking to establish core case management functionalities with additional components. End-to-end solutions will increasingly be used by smaller firms with less complex data and customer requirements.

While the new players are unlikely to challenge incumbents in their core area of case management, they are increasingly likely to attack the 'edges' of their capabilities, in areas such as transaction monitoring, entity resolution and segmentation analytics.

Finally, as AML moves beyond its core compliance areas, solution vendors are having to consider ancillary sectors where it is relatively immature, such as trade finance, gambling and the burgeoning FinTech sector (with technology companies providing financial services). While these areas offer new opportunities, they also bring their own challenges and impacts for the vendor landscape, in addressing the wide range of firms and requirements they contain.

Demand-side takeaways

FIs remain concerned about AML sanctions and fines, and not just for actual breaches. Failure to act on prior warnings can also lead to hefty penalties. The global strength of the dollar means that US regulators – with the potential to deny access to dollar swaps or the SWIFT[1] network (or both) – are among the most feared. Among US financial crime and sanctions monitoring bodies, the New York Department of Financial Services (NYDFS) has been relatively aggressive in penalizing non-US firms. But it is not unique – in March 2018 the Federal Reserve urged the

[1] *The Society for Worldwide Interbank Financial Telecommunication.*

© Copyright Infopro Digital Services Limited 2020. All Rights Reserved

Industrial and Commercial Bank of China (ICBC) to improve its AML controls; two months later the bank was hit with a fine of $5.3 million from the Financial Industry Regulatory Authority (FINRA)[2].

As part of their AML process FIs must now monitor their correspondents and subsidiaries with the same level of diligence as they use for their primary business lines. Sensitivity to AML compliance has led some FIs to sever many of their correspondent banking relationships, cutting clients and shifting their business focus from global to regional, and to territories where they are comfortable taking on risk.

Against this background, three trends are changing the AML market and vendor landscape:

- As AML software components are embedded in areas of the business outside compliance, FIs are looking for ways to reconfigure pre-existing AML processes, to drive more value from them and/or make them more efficient.

- For risk-averse FIs facing heavy regulatory pressure, using advanced analytics is becoming an area of increasing uncertainty. The success of an AML system is usually measured by the amount of time it saves and its reduction of false positives. Fearing an adverse reaction from regulators, however, FIs are reluctant to lower their SARs levels or try new technology solutions. So false positives remain high and true positives elusive. This situation creates challenges in the use of advanced analytics, and in particular machine learning (ML).

- AML requirements and capabilities are moving into adjacent sectors and industries, notably trade finance, gambling, and the FinTech sector.

    - Trade-based money laundering has a genuine impact on FIs, which lose business if they cannot confirm KYC capabilities with their trading counterparties.

    - In recent years, fines issued to gambling and gaming companies for AML-related violations have increased exponentially, and are unlikely to drop significantly, not least because the underlying market is set to expand.

    - As FinTech firms become more established across the financial services value chain, they look likely to mirror existing FIs in terms of their structure. As a result, their AML requirements are likely to resemble those of incumbent FIs.

Supply-side takeaways

Many vendors provide AML as part of their solution set, because AML components are increasingly incorporated into a wide range of processes (including operational processes such as KYC and CLM). Incumbent and established providers tend to dominate among specialist AML and sanctions solutions providers, and the combination of analytics challenges and FIs' low risk appetites means that 'trusted' vendors have significant and durable market presence.

The market changes outlined in the previous section – especially the growing challenge of analytics and AML's move into other sectors – are driving changes in the relevant technology. Much of the change in the AML marketplace comes in areas such as the adoption of innovative analytics and model risk management, and the services and technology mixtures of the vendors.

Much of FIs' AML expenditure typically goes to services firms, so a question facing many vendors is how to balance services and technology, and how to divide the human elements of their offerings from the technological ones. A firm that provides only technology components, and which relies on partners or third parties to provide services for an AML project, risks missing out on efficiencies and synergies between services and technology (depending on the services teams' familiarity with the technology, for example, or how it can be reconfigured). Conversely, a firm that offers services opens itself up to 'scope creep', and to shouldering the ballooning costs of implementation.

[2] **http://www.finra.org/newsroom/2018/finra-fines-icbcfs-53-million-anti-money-laundering-compliance-deficiencies-and-other**

© Copyright Infopro Digital Services Limited 2020. All Rights Reserved

2. Quadrant context

Introducing the Chartis RiskTech Quadrant®

This section of the report contains:

- The Chartis RiskTech Quadrant® for AML/watchlist monitoring solutions, 2019.
- An examination of Oracle's positioning and its scores as part of Chartis' analysis.
- A consideration of how the quadrant reflects the broader vendor landscape.

Summary information

What does the Chartis quadrant show?

The RiskTech Quadrant® uses a comprehensive methodology that involves in-depth independent research and a clear scoring system to explain which technology solutions meet an organization's needs. The RiskTech Quadrant® does not simply describe one technology option as the best AML/watchlist monitoring solution; rather it has a sophisticated ranking methodology to explain which solutions are best for specific buyers, depending on their implementation strategies.

The RiskTech Quadrant® is a proprietary methodology developed specifically for the risk technology marketplace. It takes into account vendors' product, technology and organizational capabilities. Section 4 of this report sets out the generic methodology and criteria used for the RiskTech Quadrant®.

How are quadrants used by technology buyers?

Chartis' RiskTech and FinTech quadrants provide a view of the vendor landscape in a specific area of risk, financial and/or regulatory technology. We monitor the market to identify the strengths and weaknesses of different solutions, and track the post-sales performance of companies selling and implementing these systems. Users and buyers can consult the quadrants as part of their wider research when considering the most appropriate solution for their needs.

Note, however, that Chartis Research does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Chartis Research's publications consist of the opinions of its research analysts and should not be construed as statements of fact.

How are quadrants used by technology vendors?

Technology vendors can use Chartis' quadrants to achieve several goals:

- Gain an independent analysis and view of the provider landscape in a specific area of risk, financial and/or regulatory technology.
- Assess their capabilities and market positioning against their competitors and other players in the space.
- Enhance their positioning with actual and potential clients, and develop their go-to-market strategies.

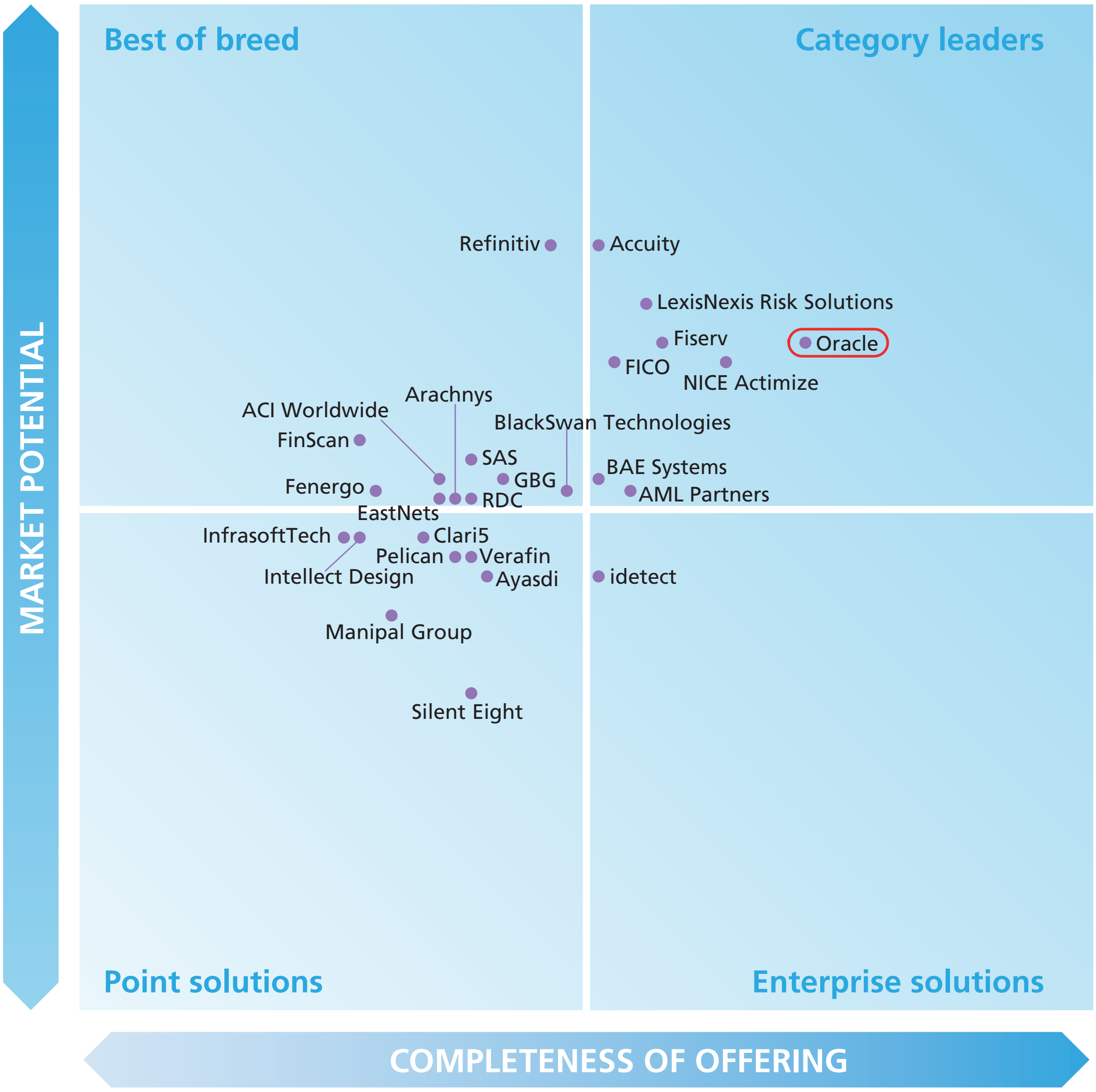
In addition, Chartis' Vendor Analysis reports, like this one, offer detailed insight into specific vendors and their capabilities, with further analysis of their quadrant positioning and scoring.

Chartis Research RiskTech Quadrant® for AML/watchlist monitoring solutions, 2019

Figure 1 illustrates Chartis' view of the AML/watchlist monitoring vendor landscape, highlighting Oracle's position.

© Copyright Infopro Digital Services Limited 2020. All Rights Reserved

Figure 1: RiskTech Quadrant® for AML/watchlist monitoring solutions, 2019



Source: Chartis Research

Quadrant Dynamics

General quadrant takeaways

AML is a component of a wide range of processes, including nominally 'operational' processes such as KYC and CLM. There are therefore a wide range of vendors that provide AML as at least part of their solution set. Beyond this, there are specialist AML and sanctions firms: this remains an area dominated by incumbents. The combination of challenging analytics and low risk appetites means that 'trusted' vendors have significant and durable market presence – if most FIs in a given geography tend to use a single vendor, then that vendor is often viewed as reliable. These firms (which include a number of vendors clustered in the upper-right of the quadrant) often have market-leading positions.

Many are packaged solution firms, which typically have powerful case management and workflow capabilities, which enable tasks to be defined and distributed to users. These vendors often lead the way in establishing robotic process automation (RPA) capabilities. Oracle has established a strong presence with RPA and case management functionality, and has also displayed strength in advanced analytical tools such as graph analytics.

© Copyright Infopro Digital Services Limited 2020. All Rights Reserved

The other market-leading incumbents tend to be data-provision firms, which offer sanctions screening and user data. Data-provision vendors are more durable, benefiting from a wide network that can help them build data science teams for validation and modeling that can then be repurposed to address data and services. While they are typically less strong in terms of pure analytics, they often have a strong market presence.

Vendor positioning in context – completeness of offering

Oracle provides a deep set of features for managing AML and watchlist monitoring. It includes customer screening with its own in-house matching algorithm and coverage of major commercial watchlists. Other areas of interest such as trade-based money laundering (a significant growth area) are also included. The ability to integrate trade-based money laundering with transaction screening, RPA and text analytics (analyzing SWIFT messages for information about ports and goods, for example) is a particular differentiator. Regulatory compliance and controls are another strength, and include out-of-the-box templates and customizable dashboarding. Oracle has also built out its already strong case management capabilities with AML event scoring and automated case decisioning within its FCC studio offering.

One area of financial crime risk analytics in which there has been notable expansion is graph analytics; Oracle has developed a robust solution in this area with its PGX graph analytics engine. Artificial intelligence (AI) capabilities have also been deployed within the Oracle AML solution stack, including validation, benchmarking and monitoring capabilities.

Table 1 shows Chartis' rankings for Oracle's coverage against each of the completeness of offering criteria.

Table 1: Completeness of offering – Oracle (AML and watchlist monitoring solutions, 2019)

Completeness of offering criterion	Coverage
Name and transaction screening capabilities	Medium
Breadth of name screening sources offered	Medium
Transaction monitoring capabilities	Medium
Regulatory compliance reporting and controls	High
Alert/case management	High
Advanced analytics	High
Visualizations and dashboarding	Medium

Source: Chartis Research

Vendor positioning in context – market potential

Oracle's Oracle Financial Services Analytical Applications (OFSAA) is a leading offering within the AML landscape, building on the historic strength of the vendor's Mantas platform. Oracle's Financial Services Crime and Compliance (FCC) Studio has enjoyed strong uptake across several geographies. The company has also consolidated its presence with a strong partnership program, which includes building out relationships with other vendors for RPA, EDD and negative news capabilities. In focusing on the higher end of the marketplace (Tier 1 and Tier 2 institutions), Oracle's value proposition is typically sold to clients that favour the sophistication of its solution, depth of experience and analytical strengths.

Table 2 shows Chartis' rankings for Oracle's coverage against each of the market potential criteria.

Table 2: Market potential – Oracle (AML and watchlist monitoring solutions, 2019)

Market potential criterion	Coverage
Customer satisfaction	Medium
Market penetration	Medium
Growth strategy	High
Financials	High

Source: Chartis Research

© Copyright Infopro Digital Services Limited 2020. All Rights Reserved

3. Vendor context

Overview of relevant solutions/ capabilities

Table 3 gives an overview of Oracle and its AML/ watchlist monitoring solution.

Oracle's FCCM product portfolio provides a wide range of AML capabilities across the value chain – as well as comprehensive data management and advanced analytics capabilities – designed from the bottom up to meet FIs' requirements (see Figure 2).

Its key capabilities include:

Customer/name screening

Comprehensive screening of prospect/customer data against lists of sanctioned individuals and companies, politically exposed persons (PEPs), known associates, and other lists of high-risk individuals and organizations. Uses out-of-the-box integration with key industry-acknowledged watchlists, and can be configured to internal watchlists.

Know Your Customer (KYC)

Assesses the risks posed by prospects by leveraging information sources that include static data, screening results, adverse-media hits, network analysis, and previous SAR and currency transaction report (CTR) filings. Powered by a comprehensive customer risk-scoring engine, the software helps institutions meet diverse KYC regulatory requirements and improve overall customer relationships.

Transaction monitoring

Automated surveillance of financial activity and customer risk to transparently detect and investigate potentially high-risk money-

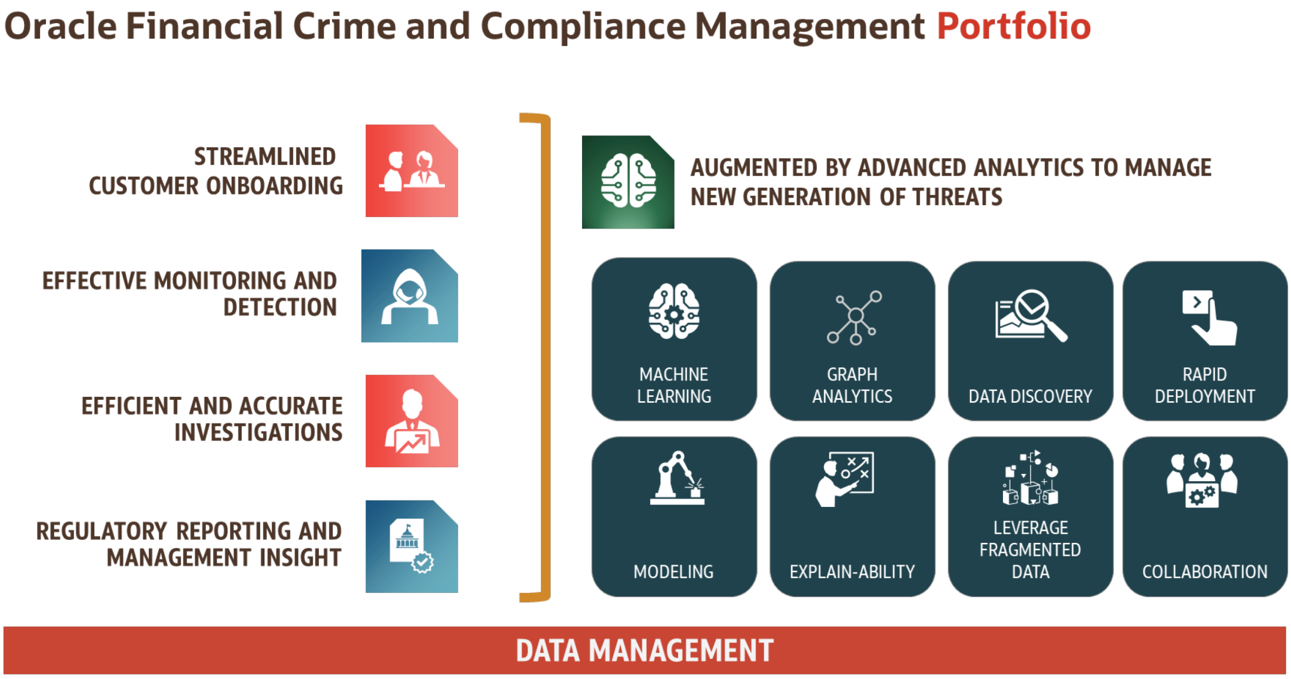
Table 3: Oracle – company information

Company	Oracle Corporation
Headquarters	Redwood City, CA, US
Description	Oracle Corporation is an American multinational computer technology firm that develops and provides database software and technology, cloud-engineered systems, and enterprise software products – particularly its own brands of database management systems – to a wide variety of industries worldwide.
Solution	Oracle's Financial Crime and Compliance Management (FCCM) suite is a comprehensive and extensible suite of applications designed to address end-to-end business requirements across the AML financial crime and compliance management value chain. Drawing on over 20 years of experience in providing crime and compliance management solutions to large banks, Oracle FCCM aims to help FIs eliminate financial crime while still ensuring operational efficiency. FCCM's key offerings span the value chain, and include: • Customer onboarding. • Monitoring and detection. • Investigations. • Regulatory reporting and management insight. These features are augmented by data management and advanced analytics capabilities.

Source: Oracle

© Copyright Infopro Digital Services Limited 2020. All Rights Reserved

Figure 2: The Oracle FCCM portfolio


Oracle Financial Crime and Compliance Management Portfolio
STREAMLINED CUSTOMER ONBOARDING
EFFECTIVE MONITORING AND DETECTION
EFFICIENT AND ACCURATE INVESTIGATIONS
REGULATORY REPORTING AND MANAGEMENT INSIGHT
AUGMENTED BY ADVANCED ANALYTICS TO MANAGE NEW GENERATION OF THREATS
MACHINE LEARNING
GRAPH ANALYTICS
DATA DISCOVERY
RAPID DEPLOYMENT
MODELING
EXPLAIN-ABILITY
LEVERAGE FRAGMENTED DATA
COLLABORATION
DATA MANAGEMENT

Source: Oracle

laundering activities and related behaviors. A unified compliance platform, it covers banking, capital markets and insurance industries. Its comprehensive library, which contains hundreds of industry-proven regulator-approved behavior-detection models, enables scenario- and profile-based detection with advanced peer-group profiling.

Transaction filtering

Real-time screening of suspicious transactions against up-to-date watchlists to mark sanctioned individuals, entities, accounts, vessels, ports, cities, stop keywords, countries, etc. The software can be integrated out-of-the-box with industry watchlists, and is configurable with internal watchlists. It can also enable users to adjudicate blocked transactions within minutes to help boost investigators' productivity.

Centralized case management

A single enterprise-wide platform that consolidates events from across monitoring solutions, Oracle Enterprise Case Management can help FIs meet the diverse demands of financial-crime investigation functions. Integrated correlation and event-scoring capabilities help to give users a true risk-based approach to prioritizing events. With this firms can automatically share channel-specific intelligence to collaborate with analysts across enterprise investigation units; enforce consistent investigation process workflows; and ensure that key performance indicators (KPIs) are attained to enable the timely closure of alerts and the submission of SARs.

Advanced analytics

Oracle continues to invest in innovating its advanced analytics to augment traditional AML engines, to help make them more effective and efficient in the changing financial crime landscape. Key capabilities include:

- An integrated analytics workbench with graph analytics, data visualization, machine learning, scenario authoring and testing capabilities for financial crime data. Equipped with secure access to production data, pre-defined scenarios, and out-of-the-box graph queries and visualizations.

- Real-time event risk-scoring engine with algorithmic scoring models for accurate customer risk assessment.

- A platform to augment rule-based models with machine-based behavioral models, using 300+

© Copyright Infopro Digital Services Limited 2020. All Rights Reserved

highly relevant AML attributes and automated modeling tasks.

- Inbuilt graph analytical tools for advanced entity resolution, network pattern analysis, deep learning and the discovery of hidden network patterns.
- Natural language processing for enhanced feature engineering.
- Automated threshold tuning to help users arrive at optimum threshold levels.

Regulatory reporting

Comprehensive out-of-the-box reporting templates are coupled with automated workflows that meet regulatory reporting needs across jurisdictions (such as SAR, CTR, and Foreign Account Tax Compliance Act [FATCA]/GoAML filings).

Management insights

Business intelligence and analytical reporting, providing clear operational visibility into the performance of FIs' compliance programs.

Vendor leading practices

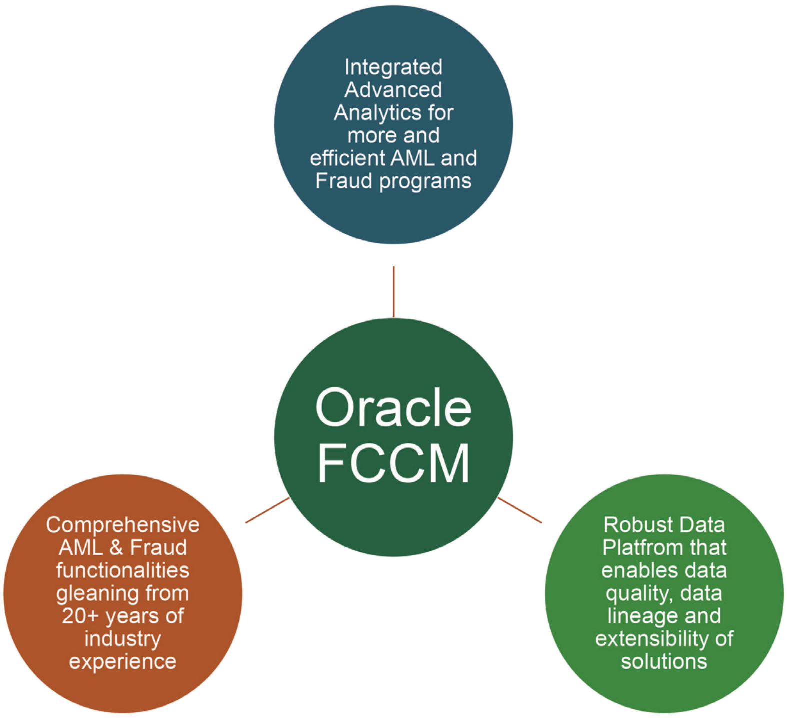
The Oracle FCCM portfolio allows institutions to monitor, detect, investigate and report complex suspicious money movement transactions across products and channels (see Figure 3).

The portfolio has been constantly upgraded with technologies (such as advanced analytics) to enable it to keep pace with the changing patterns and increasing complexities of financial crime. With Oracle's FCCM portfolio, FIs can continue to use their existing rule-based models, and adopt capabilities including entity resolution, machine-learning-based model creation, graph-based detection and network pattern investigations, and supervised and unsupervised learning. The solution's inbuilt financial crime data platform enables FIs to bridge existing gaps in rules-based paradigms and move toward adopting advanced analytics capabilities in their AML programs.

The Oracle FCCM platform enables organizations to adopt innovations at scale by overcoming challenges around:

- The acquisition, transformation and quality of data.

Figure 3: Key components of Oracle's FCCM portfolio


Integrated Advanced Analytics for more and efficient AML and Fraud programs
Oracle FCCM
Comprehensive AML & Fraud functionalities gleaning from 20+ years of industry experience
Robust Data Platfrom that enables data quality, data lineage and extensibility of solutions

Source: Oracle

- Regulatory acceptance of detection scenarios and models.
- Operationalizing advanced analytics on top of core AML processes.

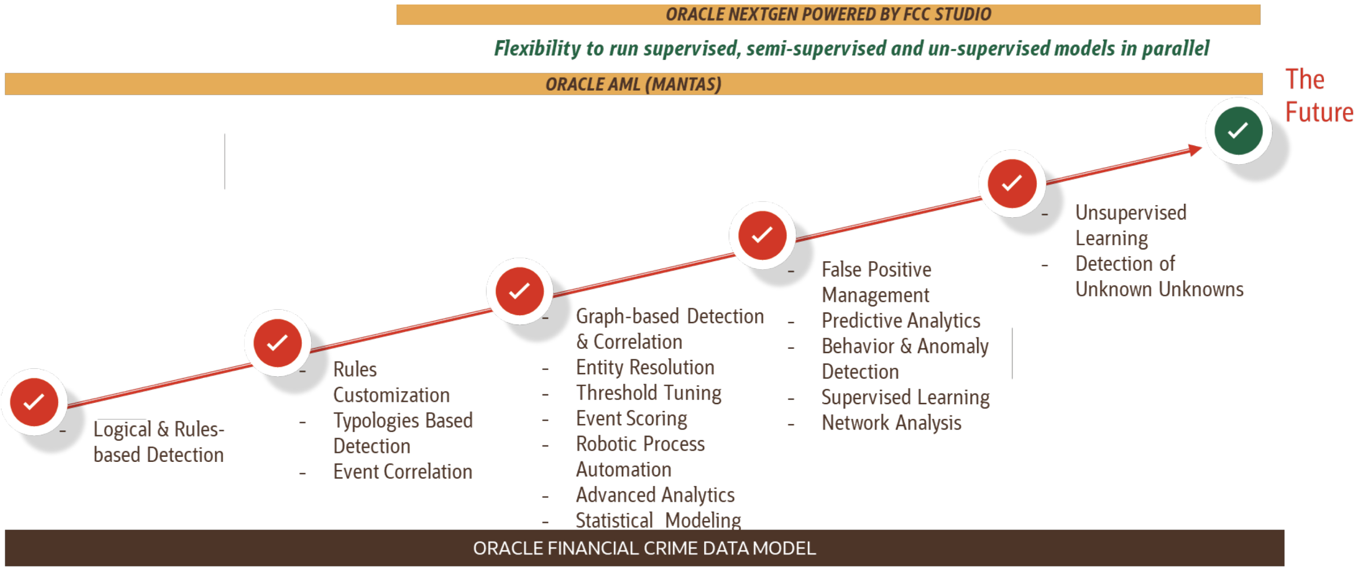
It achieves this by:

- Staging all Oracle FCCM applications on a common financial crime data model that is system-agnostic, and which can leverage data from any transaction monitoring system (see Figure 4). Tight integration of applications across the value chain, via a common platform, makes it easier to transform and consume data in advanced analytics applications for monitoring, detection and investigations, and to operationalize applications for core AML processes.
- Oracle's modelXray (explainable AI) functionality helps to bring transparency and insight into sophisticated machine learning models, bringing them one step closer to regulatory acceptance.

Oracle provides comprehensive AML capabilities across the value chain, complemented by integrated advanced analytics and a robust data management platform to support its solutions (see Figure 5).

© Copyright Infopro Digital Services Limited 2020. All Rights Reserved

Figure 4: Enabling frictionless transition to the future of financial crime and compliance management

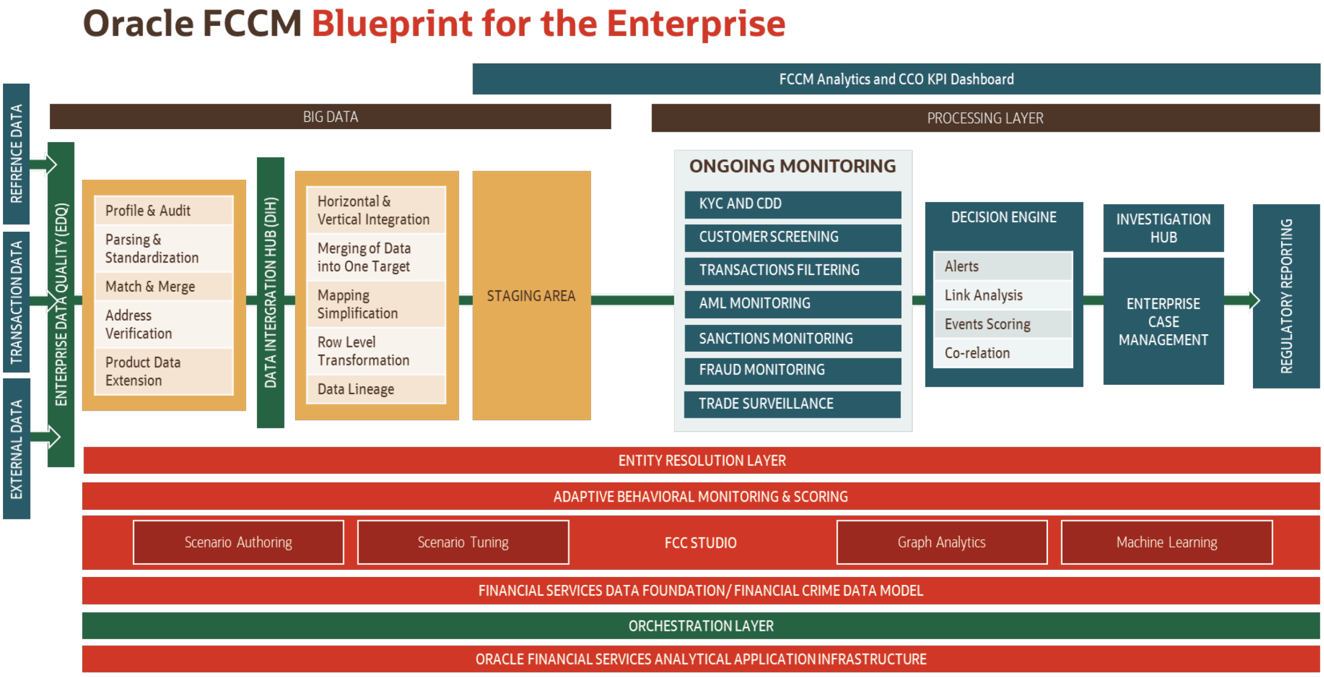

ORACLE NEXTGEN POWERED BY FCC STUDIO
Flexibility to run supervised, semi-supervised and un-supervised models in parallel
ORACLE AML (MANTAS)
The Future
- Logical & Rules-based Detection
- Rules Customization
- Typologies Based Detection
- Event Correlation
- Graph-based Detection & Correlation
- Entity Resolution
- Threshold Tuning
- Event Scoring
- Robotic Process Automation
- Advanced Analytics
- Statistical Modeling
- False Positive Management
- Predictive Analytics
- Behavior & Anomaly Detection
- Supervised Learning
- Network Analysis
- Unsupervised Learning
- Detection of Unknown Unknowns
ORACLE FINANCIAL CRIME DATA MODEL

Source: Oracle

In terms of its functionality, Oracle's FCCM portfolio is a one-stop-solution that addresses the range of FIs' AML regulatory compliance needs, complemented by advanced analytics covering the value chain (see Figure 6).

Streamlined customer onboarding. Oracle equips onboarding personnel with quick, useful information, complemented by analytical tools, to help them identify and mitigate risks without affecting the onboarding experience.

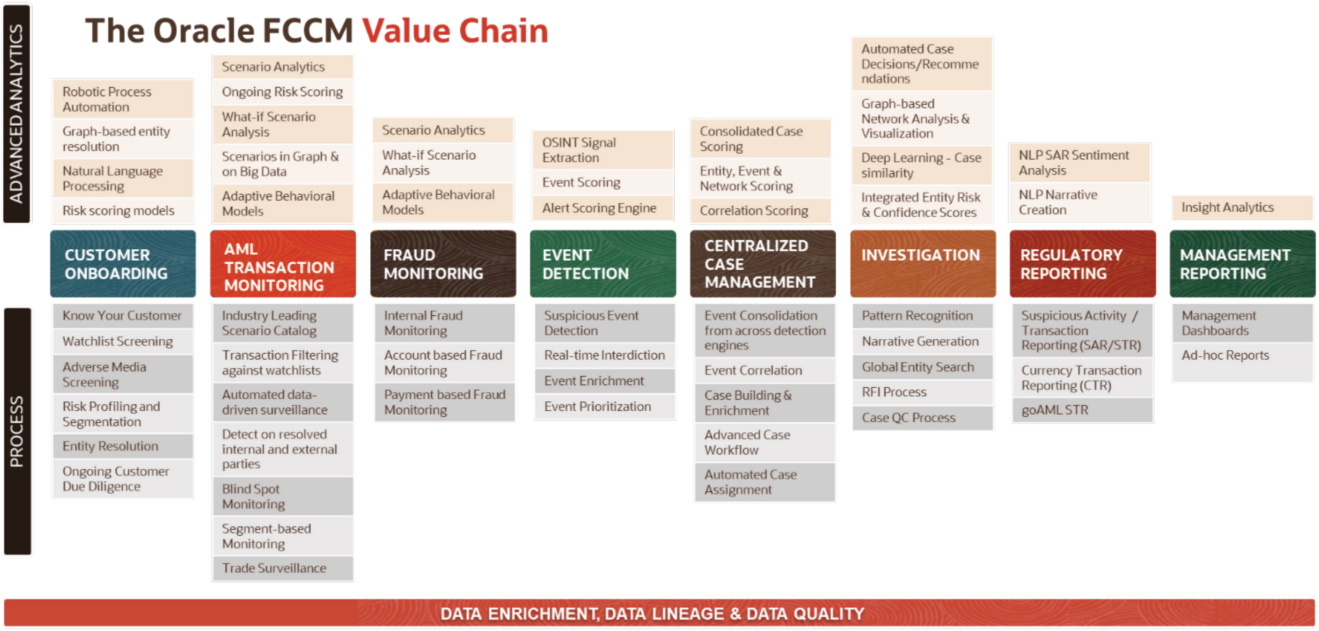
Figure 5: Oracle FCCM – a comprehensive solution



Source: Oracle

© Copyright Infopro Digital Services Limited 2020. All Rights Reserved

Figure 6: The Oracle FCCM value chain



The Oracle FCCM Value Chain

ADVANCED ANALYTICS

PROCESS

CUSTOMER ONBOARDING
Robotic Process Automation
Graph-based entity resolution
Natural Language Processing
Risk scoring models
Know Your Customer
Watchlist Screening
Adverse Media Screening
Risk Profiling and Segmentation
Entity Resolution
Ongoing Customer Due Diligence

AML TRANSACTION MONITORING
Scenario Analytics
Ongoing Risk Scoring
What-if Scenario Analysis
Scenarios in Graph & on Big Data
Adaptive Behavioral Models
Industry Leading Scenario Catalog
Transaction Filtering against watchlists
Automated data-driven surveillance
Detect on resolved internal and external parties
Blind Spot Monitoring
Segment-based Monitoring
Trade Surveillance

FRAUD MONITORING
Scenario Analytics
What-if Scenario Analysis
Adaptive Behavioral Models
Internal Fraud Monitoring
Account based Fraud Monitoring
Payment based Fraud Monitoring

EVENT DETECTION
OSINT Signal Extraction
Event Scoring
Alert Scoring Engine
Suspicious Event Detection
Real-time Interdiction
Event Enrichment
Event Prioritization

CENTRALIZED CASE MANAGEMENT
Consolidated Case Scoring
Entity, Event & Network Scoring
Correlation Scoring
Event Consolidation from across detection engines
Event Correlation
Case Building & Enrichment
Advanced Case Workflow
Automated Case Assignment

INVESTIGATION
Automated Case Decisions/Recommendations
Graph-based Network Analysis & Visualization
Deep Learning - Case similarity
Integrated Entity Risk & Confidence Scores
Pattern Recognition
Narrative Generation
Global Entity Search
RFI Process
Case QC Process

REGULATORY REPORTING
NLP SAR Sentiment Analysis
NLP Narrative Creation
Suspicious Activity / Transaction Reporting (SAR/STR)
Currency Transaction Reporting (CTR)
goAML STR

MANAGEMENT REPORTING
Insight Analytics
Management Dashboards
Ad-hoc Reports

DATA ENRICHMENT, DATA LINEAGE & DATA QUALITY

Source: Oracle

- Centralized 360° management of customers, with automated screening against sanctions lists, PEP watchlists, negative news, blogs, forums, etc.

- Centralized due diligence, with seamless application programming interface (API) integrations with external data sources.

- Accurate risk assessment with real-time entity scoring engine that uses algorithmic scoring models.

- Inbuilt graph-based tools for advanced discovery and entity resolution.

- Explainable risk-scoring models that are fully documented for review by internal audit or regulators.

Effective monitoring and detection. To enhance its catalog of industry-proven, regulator-approved AML and fraud scenarios, the company has used ML to address FIs' twin needs of increasing the effectiveness of detection and improving model explainability. The modelXray functionality also helps to bring transparency and insight to sophisticated black-box machine models.

Key advanced capabilities used to enhance the effectiveness of detection include:

- An interactive workbench platform that enables data scientists and pattern miners to formulate queries, productize them, and visualize data interactively.

- The ability to augment existing rules-based models with adaptive machine-based customer behavior models to counter criminals' changing behavior patterns.

- An automated threshold tuning module, bundled with the detection system.

Efficient and accurate investigations. The efficiency of investigations and the productivity of investigators have an impact on a firm's regulatory compliance and its bottom line. The steps Oracle has taken in this area include:

- Providing a 360° view of customers, transactions, related events, parties, and any matching external data.

- Graph analytics tools with intuitive visual network depiction, to uncover hidden criminal patterns.

- Integrated event scoring to enable a risk-based approach by prioritizing events with the highest probability of risk.

© Copyright Infopro Digital Services Limited 2020. All Rights Reserved

- Relationship discovery and repetitive-behavior pattern recognition between business entities and across historical investigations.
- Investigation dashboards with analytical insights and recommendations for next-best actions.

Regulatory reporting and management insights provided by the solution include:

- Out-of-the-box AML/CFT reporting templates to meet regulatory reporting requirements across key global jurisdictions.
- Periodic updates to ensure that capabilities continually conform to regulatory and tax compliance reporting needs.
- Business intelligence and analytical reporting, providing clear operational visibility into the performance of FIs' compliance programs.

Addressing the needs of smaller banks. To address the AML compliance needs of smaller banks, Oracle has released a new end-to-end AML application with integrated case management capabilities. This new AML product is cost-effective, and can be easily implemented on the cloud or on-premise. Its user-friendly interface enables drag-and-drop data pipeline creation and maintenance, as well as scenario authoring and maintenance. This eliminates the need for additional operational costs around data management and scenario development.

From a technology perspective, the key functionality of Oracle's FCCM platform can be distilled down to three major capabilities:

- **An enterprise approach to unified financial crime data management**. A robust data model and comprehensive data management foundation underpin all Oracle's FCCM applications. Building on tools such as Oracle Enterprise Data Quality, Data Integration Hub and Oracle Enterprise Metadata Manager, the platform can provide a rich set of data quality, lineage and dimension management frameworks.
- In addition to tools, FCCM applications are built on **a common data model** – the Oracle Financial Crime Data Management Framework. The Financial Services Data Model is standardized across customers, enabling Oracle's product-centric approach.
- **Intelligent, open and extensible**. The open, extensible platform supports external analytical engines, applications, and models developed internally or acquired from third parties. Simplified data access for all lines of business, organizational units and geographic regions helps to bridge the gap between financial crime analytics and investigations.
- Oracle's **product-centric approach** enables users to upgrade to the newest releases, and to clone and deploy the same software globally, across multiple jurisdictions.
- **State-of-the-art technical infrastructure**. The technology platform for the FCCM portfolio is built on leading-edge analytics infrastructure such as Apache Spark, Oracle Parallel Graph Engine, and Oracle Exadata.
- **Oracle's investments** in AI and ML (Oracle Advanced Analytics for Hadoop and Oracle R enterprise); scalable graph analytics (Oracle Parallel Graph Engine); enterprise data quality tools (EDQ); Big Data (Big Data Adaptors for Oracle database); and engineered systems (Oracle Exadata) are fully utilized in the FCCM platform.

The Oracle FCCM suite has been architected to be multi-tiered and open-systems compliant. Its component-based architecture aims to maximize performance, openness and extensibility; FCCM can be configured in one, two or more tiers as required, and is fully web-enabled.

© Copyright Infopro Digital Services Limited 2020. All Rights Reserved

4. Methodology

Overview

Chartis is a research and advisory firm that provides technology and business advice to the global financial services industry. Chartis provides independent market intelligence regarding market dynamics, regulatory trends, technology trends, best practices, competitive landscapes, market sizes, expenditure priorities, and mergers and acquisitions. Chartis' RiskTech and FinTech Quadrant™ reports are written by experienced analysts with hands-on experience of selecting, developing and implementing financial technology solutions for a variety of international companies in a range of industries including banking, insurance and capital markets. The findings and analyses in our quadrant reports reflect our analysts' considered opinions, along with research into market trends, participants, expenditure patterns, and best practices.

Chartis seeks to include RiskTech and FinTech vendors that have a significant presence in a given target market. The significance may be due to market penetration (e.g., a large client base) or innovative solutions. Chartis uses detailed 'vendor evaluation forms' and briefing sessions to collect information about each vendor. If a vendor chooses not to respond to a Chartis request for information, Chartis may still include the vendor in the report. Should this happen, Chartis will base its opinion on direct data collated from technology buyers and users, and from publicly available sources.

Chartis' research clients include leading financial services firms and Fortune 500 companies, leading consulting firms and financial technology vendors. The vendors evaluated in our quadrant reports can be Chartis clients or firms with whom Chartis has no relationship.

Chartis evaluates all vendors using consistent and objective criteria, regardless of whether or not they are Chartis clients. Chartis does not give preference to its own clients and does not request compensation for inclusion in a quadrant report, nor can vendors influence Chartis' opinion.

Selection criteria

In selecting vendors for this report, we aimed to give a representative view of the landscape and its main categories of incumbent vendors, packaged solution vendors and data solution firms, as well as emerging firms. We also selected vendors that provide AML as part of their solution set, because AML components are increasingly incorporated into a wide range of processes (including operational processes such as KYC and CLM).

This year we also decided to combine the watchlist monitoring and AML quadrants, so vendors offering solutions from both areas received higher completeness of offering scores. We also took a component approach to our market analysis, looking at any vendors that provided an element of transaction monitoring and name-screening capabilities.

Briefing process

We conducted face-to-face and/or web-based briefings with each vendor[3]. During these sessions, Chartis experts asked in-depth, challenging questions to establish the real strengths and weaknesses of each vendor. Vendors provided Chartis with:

- A business update – an overview of solution sales and client satisfaction.
- A product update – an overview of relevant solutions and R&D roadmaps.
- A product demonstration – key differentiators of their solutions relative to those of their competitors.

In addition to briefings, Chartis used other third-party sources of data, such as conferences, academic and regulatory studies, and publically available information.

Evaluation criteria

We develop specific evaluation criteria for each piece of quadrant research from a broad range of overarching criteria, outlined below. By using domain-specific criteria relevant to each individual risk, we can ensure transparency in our methodology, and allow readers to fully appreciate the rationale for our analysis. The specific criteria

[3] *Note that vendors do not always respond to requests for briefings; they may also choose not to participate in the briefings for a particular report.*

© Copyright Infopro Digital Services Limited 2020. All Rights Reserved

used for AML/watchlist monitoring are shown in Table 4.

Table 4: Evaluation criteria for Chartis' AML/watchlist monitoring report

Completeness of offering	Market potential
Name and transaction screening capabilities	Customer satisfaction
Breadth of name screening sources offered	Market penetration
Transaction monitoring capabilities	Growth strategy
Regulatory compliance reporting and controls	Financials
Alert/case management	
Advanced analytics	
Visualizations and dashboarding	

Source: Chartis Research

Completeness of offering

- **Depth of functionality**. The level of sophistication and amount of detailed features in the software product (e.g., advanced risk models, detailed and flexible workflow, domain-specific content). Aspects assessed include: innovative functionality, practical relevance of features, user-friendliness, flexibility, and embedded intellectual property. High scores are given to those firms that achieve an appropriate balance between sophistication and user-friendliness. In addition, functionality linking risk to performance is given a positive score.

- **Breadth of functionality**. The spectrum of requirements covered as part of an enterprise risk management system. This will vary for each subject area, but special attention will be given to functionality covering regulatory requirements, multiple risk classes, multiple asset classes, multiple business lines, and multiple user types (e.g. risk analyst, business manager, CRO, CFO, Compliance Officer). Functionality within risk management systems and integration between front-office (customer-facing) and middle/back office (compliance, supervisory and governance) risk management systems are also considered.

- **Data management and technology infrastructure**. The ability of risk management systems to interact with other systems and handle large volumes of data is considered to be very important. Data quality is often cited as a critical success factor and ease of data access, data integration, data storage, and data movement capabilities are all important factors. Particular attention is given to the use of modern data management technologies, architectures and delivery methods relevant to risk management (e.g., in-memory databases, complex event processing, component-based architectures, cloud technology, and Software as a Service). Performance, scalability, security and data governance are also important factors.

- **Risk analytics**. The computational power of the core system, the ability to analyze large amounts of complex data in a timely manner (where relevant in real time), and the ability to improve analytical performance are all important factors. Particular attention is given to the difference between 'risk' analytics and standard 'business' analytics. Risk analysis requires such capabilities as non-linear calculations, predictive modeling, simulations, scenario analysis, etc.

- **Reporting and presentation layer**. The ability to present information in a timely manner, the quality and flexibility of reporting tools, and ease of use, are important for all risk management systems. Particular attention is given to the ability to do ad-hoc 'on-the-fly' queries (e.g., 'what-if' analysis), as well as the range of 'out of the box' risk reports and dashboards.

Market potential

- **Business model**. Includes implementation and support and innovation (product, business model and organizational). Important factors include size and quality of implementation team, approach to software implementation, and post-sales support and training. Particular attention is given to 'rapid' implementation methodologies and 'packaged' services offerings. Also evaluated are new ideas, functionality and technologies to solve specific risk management problems. Speed to market, positioning, and translation into incremental revenues are also important success factors in launching new products.

- **Market penetration**. Volume (i.e. number of customers) and value (i.e. average deal size) are considered important. Rates of growth relative to sector growth rates are also evaluated. Also covers brand awareness, reputation, and the ability to leverage current market position to

© Copyright Infopro Digital Services Limited 2020. All Rights Reserved

expand horizontally (with new offerings) or vertically (into new sectors).

- **Financials**. Revenue growth, profitability, sustainability, and financial backing (e.g. the ratio of license to consulting revenues) are considered key to scalability of the business model for risk technology vendors.

- **Customer satisfaction**. Feedback from customers is evaluated, regarding after-sales support and service (e.g. training and ease of implementation), value for money (e.g. price to functionality ratio) and product updates (e.g. speed and process for keeping up to date with regulatory changes).

- **Growth strategy**. Recent performance is evaluated, including financial performance, new product releases, quantity and quality of contract wins, and market expansion moves. Also considered are the size and quality of the sales force, sales distribution channels, global presence, focus on risk management, messaging, and positioning. Finally, business insight and understanding, new thinking, formulation and execution of best practices, and intellectual rigor are considered important.

Quadrant construction process

Chartis constructs its quadrants after assigning scores to vendors for each component of the Completeness of Offering and Market Potential criteria. By aggregating these values, we produce total scores for each vendor on both axes, which are used to place the vendor on the quadrant.

Definition of quadrant boxes

Chartis' quadrant reports do not simply describe one technology option as the best solution in a particular area. Our ranking methodology is designed to highlight which solutions are best for specific buyers, depending on the technology they need and the implementation strategy they plan to adopt. Vendors that appear in each quadrant have characteristics and strengths that make them especially suited to that particular category, and by extension to particular users' needs.

Point solutions

- Point solutions providers focus on a small number of component technology capabilities, meeting a critical need in the risk technology market by solving specific risk management problems with domain-specific software applications and technologies.

- They are often strong engines for innovation, as their deep focus on a relatively narrow area generates thought leadership and intellectual capital.

- By growing their enterprise functionality and utilizing integrated data management, analytics and Business Intelligence (BI) capabilities, vendors in the point solutions category can expand their completeness of offering, market potential and market share.

Best-of-breed

- Best-of-breed providers have best-in-class point solutions and the ability to capture significant market share in their chosen markets.

- They are often distinguished by a growing client base, superior sales and marketing execution, and a clear strategy for sustainable, profitable growth. High performers also have a demonstrable track record of R&D investment, together with specific product or 'go-to-market' capabilities needed to deliver a competitive advantage.

- Because of their focused functionality, best-of-breed solutions will often be packaged together as part of a comprehensive enterprise risk technology architecture, co-existing with other solutions.

Enterprise solutions

- Enterprise solution providers typically offer risk management technology platforms, combining functionally rich risk applications with comprehensive data management, analytics and BI.

- A key differentiator in this category is the openness and flexibility of the technology architecture and a 'toolkit' approach to risk analytics and reporting, which attracts larger clients.

- Enterprise solutions are typically supported with comprehensive infrastructure and service capabilities, and best-in-class technology delivery. They also combine risk management content, data and software to provide an integrated 'one stop shop' for buyers.

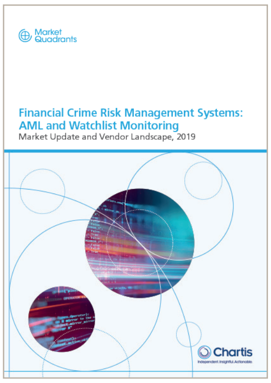
© Copyright Infopro Digital Services Limited 2020. All Rights Reserved

Category leaders

- Category leaders combine depth and breadth of functionality, technology and content with the required organizational characteristics to capture significant share in their market.
- They demonstrate a clear strategy for sustainable, profitable growth, matched with best-in-class solutions and the range and diversity of offerings, sector coverage and financial strength to absorb demand volatility in specific industry sectors or geographic regions.
- They will typically benefit from strong brand awareness, a global reach, and strong alliance strategies with leading consulting firms and systems integrators.

© Copyright Infopro Digital Services Limited 2020. All Rights Reserved

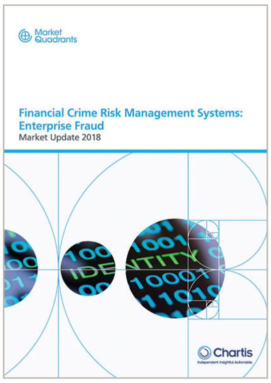
5. Further reading


Market Quadrants

Financial Crime Risk Management Systems: AML and Watchlist Monitoring
Market Update and Vendor Landscape, 2019

Chartis

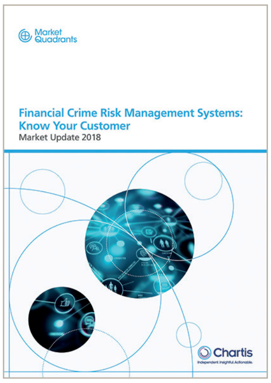
Financial Crime Risk Management Systems: AML and Watchlist Monitoring; Market Update and Vendor Landscape, 2019


Market Quadrants

Financial Crime Risk Management Systems: Enterprise Fraud
Market Update 2018

Chartis

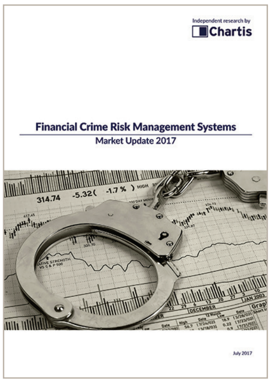
Financial Crime Risk Management Systems: Enterprise Fraud; Market Update 2018


Market Quadrants

Financial Crime Risk Management Systems: Know Your Customer
Market Update 2018

Chartis

Financial Crime Risk Management Systems: Know Your Customer; Market Update 2018


Independent research by Chartis

Financial Crime Risk Management Systems
Market Update 2017

July 2017

Financial Crime Risk Management Systems; Market Update 2017

Market Quadrants

Model validation solutions, 2019
Overview and market landscape

Chartis

Model Validation Solutions, 2019: Overview and Market Landscape

Market Insight

Global Risk IT Expenditure in Financial Services
2018 Update

Chartis

Global Risk IT Expenditure in Financial Services, 2018 Update

For all these reports, see **www.chartis-research.com**

© Copyright Infopro Digital Services Limited 2020. All Rights Reserved