



Chartis

Financial Crime and Compliance50 2024



Chartis

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 management 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.
- Wealth advisory.
- Asset management.

Chartis focuses on risk and compliance technology, giving 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 developing and implementing risk management systems and programs for Fortune 500 companies and leading consulting firms.

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

© Copyright Infopro Digital Services Limited 2024. 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 are based on information gathered in good faith, the accuracy of which we cannot guarantee. Chartis accepts no liability whatsoever 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 Trademarks of Infopro Digital Services Limited.

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

Table of contents

1. Foreword	4
2. Overview	5
3. Market view: FinCrime and compliance, 2024 and beyond	7
4. Financial Crime and Compliance50 2024 rankings	15
5. Category winners	16
6. Appendix A: Research methodology	20
7. Further reading	21

List of figures and tables

Figure 1: A truly global presence – locations of vendors who participated in the FCC50	5
Figure 2: The power of platforms	6
Figure 3: An interconnected ecosystem fueling collaboration	7
Figure 4: Estimated value of the FinCrime and compliance solution market	8
Figure 5: The requirements of modern innovation	13

1. Foreword



I'm very pleased to welcome you to the inaugural Financial Crime and Compliance50 (FCC50) ranking and report from Chartis Research. This is the first time we have ranked the vendors in the FinCrime and compliance space, a market – as we explore later in the report – likely to be worth more than \$26 billion by the end of next year.

As with our other ranking reports, our detailed analysis for FCC50 considers firms' technological advances and strategic direction to provide a complete view of how market leaders are driving transformation in this sector.

In the following pages, we discuss the broader trends and dynamics in the market. While criminals have become more advanced and use more sophisticated technology, those fighting them now have many more tools of their own. Crucially, industry players are also learning how to collaborate, communicate and innovate.

Financial institutions are not cutting their spend – but they are becoming more savvy, and have a more astute understanding of what constitutes value. They know that by leveraging technology and data insights effectively, they can strike a balance between protecting themselves and their customers and ensuring they comply with the law. Many of the tools they have just aren't up to the job, however, and/or cost too much to run, making lower cost of ownership and solution affordability increasingly critical.

Meanwhile, the drive to widen the availability of FinCrime solutions is being helped by several technological advances, including cloud hosting, containerization and no-code interfaces. And let's not forget AI – which, while a potentially big disruptor in the space, operates on the core principles of effective innovation: it must be practical, explainable and impactful.

As with all our research and rankings, with FCC50 Chartis will explore and analyze these and other trends and dynamics, bringing our clear-eyed view to this important and highly relevant market and technology space.

Finally, it just remains for me to congratulate all the featured vendors. I hope you enjoy the report.

Nick Vitchev, Research Director

2. Overview

The FCC50 ranking and report examine the landscape for compliance-led financial crime management solutions. These are solutions that enable financial institutions to understand who they are working with, their customers, their counterparties and other factors that could pose a threat to their integrity. This report aims to highlight the breadth, diversity and innovation in the market, and to shed light on some of the many vendors that excel in this space.

It covers the following disciplines and solution types:

- Anti-money laundering (AML).
- Sanctions, politically exposed person (PEP) and adverse media screening.
- Know Your Customer (KYC) systems.
- The provision, process and delivery of financial crime-related data.

Within these areas, we examine key technological innovations, enablers and facets of the ecosystem that include: core engines, platforms and orchestration, policy, analytics, reporting, packaging and delivery.

Financial crime is a truly global problem, and financial inclusion is now increasingly prominent as a market focus (see the market view section). Chartis has strived to reflect this diversity in the range of vendors we assessed (see Figure 1). However, this alone doesn't tell the full story, because the range of geographies serviced by the featured vendors greatly outnumbered their HQ locations. We were also determined to highlight a breadth of institution types, sizes and approaches, reflecting the highly diverse market firms now operate in.

Figure 1: A truly global presence – locations of vendors who participated in the FCC50



Source: Chartis Research

Fraud and FinCrime

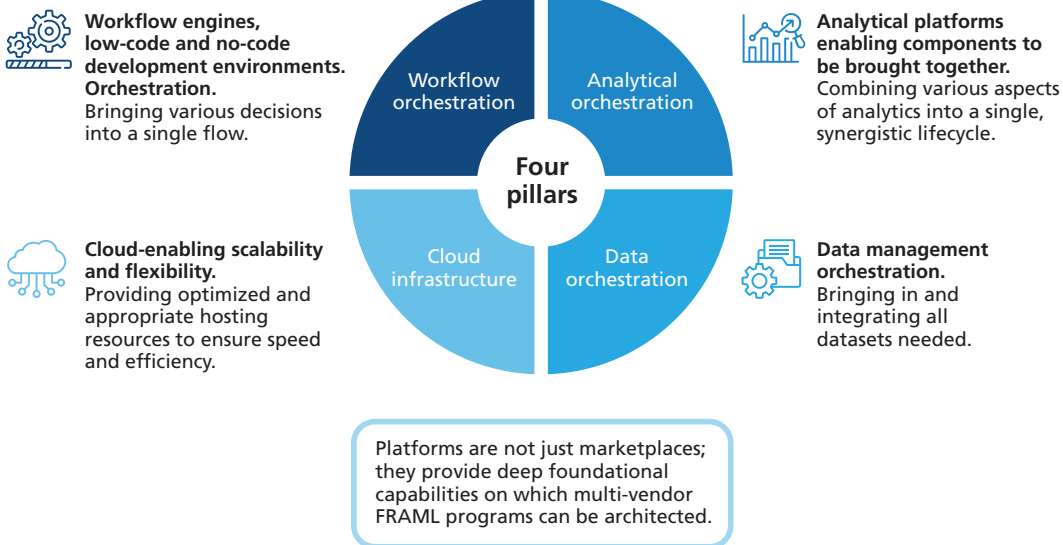
Notably absent from this report and research is fraud, a major type of financial crime. This isn't because fraud is not central to the financial crime ecosystem (it is, very much so). Nor is it that an intersection between fraud and other financial crimes doesn't exist – in fact, other crimes (such as money laundering) frequently involve fraudulent activity.

Fraud is not a central component of this report because by removing it from the rest of financial crime we can shed light on other aspects of that universe. When seeking feedback from banks, financial institutions and other organizations in the lead-up to this report, we identified an appetite among firms for analysis of compliance-led FinCrime typologies.

That said, fraud detection technology does factor into this report. Increasingly, the detection of risk typologies moves across area boundaries, and many firms now blend fraud signals with money laundering signals and other data to enrich their understanding of the threat an individual or organization may pose (see Figure 2).

Chartis explored the intersection of fraud and other financial crime typologies in its 2023 **report on FRAML**, and viewed fraud through a payments-specific lens in its **report on payment risk solutions**.

Figure 2: The power of platforms



Source: Chartis Research

3. Market view: FinCrime and compliance, 2024 and beyond

The bad news

Financial criminals have become more advanced, more sophisticated and more determined than ever. And technology in various forms is enabling them to commit more crimes, faster. For example:

- By automating profile creation to exploit gaps in KYC controls, they can set up convoluted corporate structures, shell companies or ownership models to facilitate money laundering.
- By using AI and other analytical tools to ‘industrialize’ money laundering pattern development, they can find new ways of moving money through entities with minimum risk of detection.

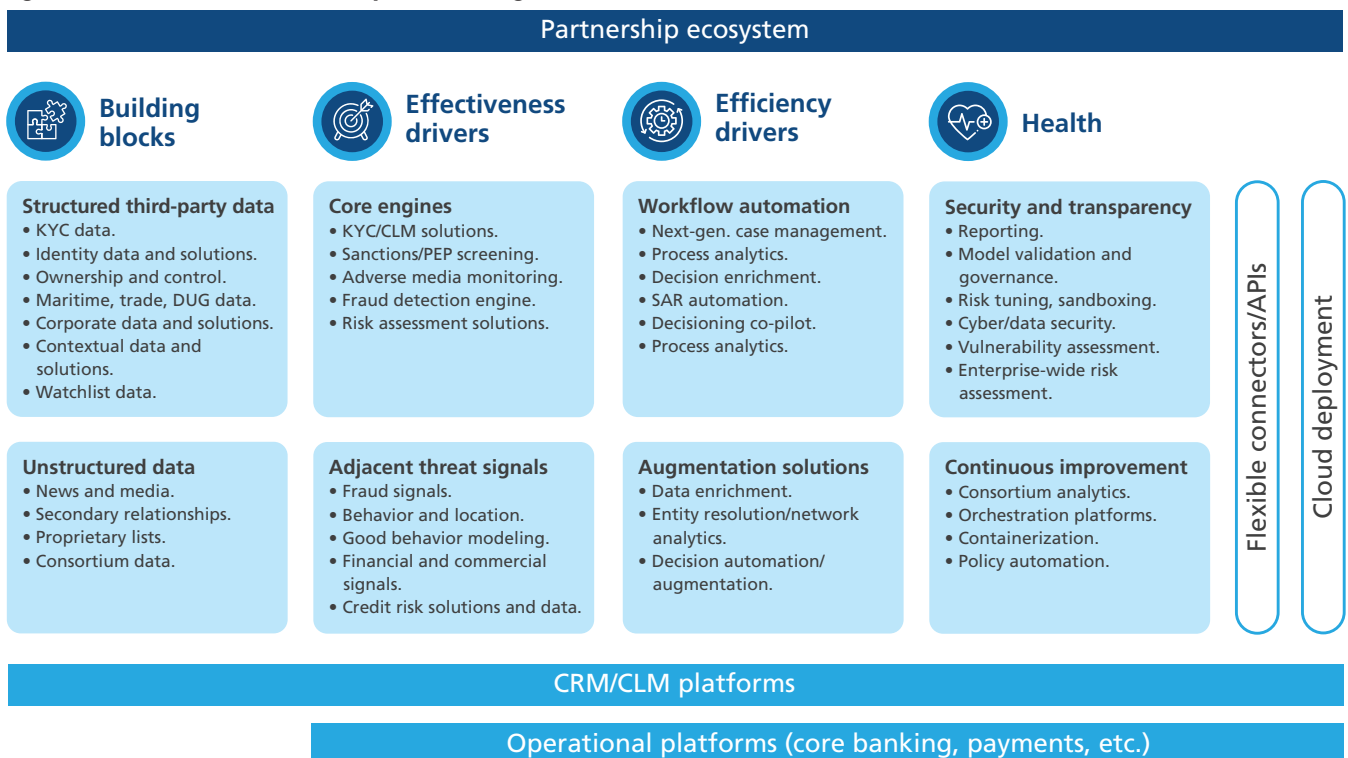
Meanwhile, communication networks, often – but not exclusively – on the dark web, are enabling global, instant communication between organized crime groups.

The cost of financial crime to the global economy is estimated at more than \$1.4 trillion a **year**, and is the tip of a very large iceberg. The trail of destruction left by financial crime on individuals, organizations and countries is immeasurable.

The good news

Despite the challenges, those fighting financial crime now have many more tools at their disposal to help them identify, prevent and report not only criminal activity but also higher-risk actors and approaches. Industry players are also learning how to collaborate and communicate, a development very much enabled by technology vendors (see Figure 3).

Figure 3: An interconnected ecosystem fueling collaboration



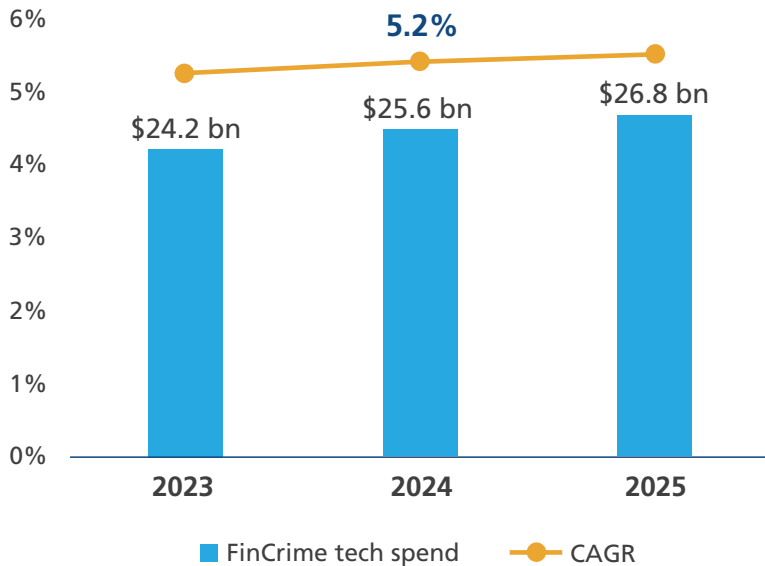
Source: Chartis Research

In addition to technology and collaboration, the third major positive shift we have seen in the past few years is the drive toward 'financial inclusion', i.e., the belief that everyone, regardless of location or situation, should be able to obtain high-performance financial crime technology. Firms' growing ability to deliver on this premise could revolutionize the market.

A growing market

As a result of these shifts and dynamics, the world of financial crime is now vast and complex, and the market for fighting it large and diverse. Chartis estimates that the financial crime and compliance market will be worth \$25.6 billion in 2024, growing from \$24.2 billion in 2023. We estimate that by the end of 2025, it will have grown by 5.2% to \$26.8 billion (see Figure 4).

Figure 4: Estimated value of the FinCrime and compliance solution market



Source: Chartis Research

Within this market we are seeing the following trends:

- Double-digit growth in spending on AML transaction monitoring systems, driven by adoption of analytics and next-generation user interfaces and case management.
- Robust investment in watchlist and KYC data management, with high single-digit growth across these markets. While growth in spend on core screening engines remains consistent yet modest, we are seeing strong double-digit growth across data enrichment and augmented analytics.
- Adverse media and related activities have become more of a priority for many financial institutions, and we are forecasting a double-digit rise in investment in this area in 2024.

Context: the dynamics of demand

So what are the drivers and dynamics in this shifting market?

End-user dynamics: what's shaping demand

Several dynamics in the market landscape are shaping current demand for FinCrime and compliance solutions. Very few institutions, whether global banks or smaller FinTechs, are unaffected by the global economic downturn. In addition, financial markets have become fiercely competitive. With this in mind, it's not surprising that a constant theme we came across in our research was around *value*. To be clear, this doesn't mean that institutions are slashing costs across the board, nor that they are looking for the cheapest option. Quite the opposite. Institutions have become a lot more sophisticated and savvy in understanding and measuring value, not only for the short term but also the longer term.

Many established tools are unwieldy and expensive to run, and as the regulatory and crime landscapes change, firms need more sophisticated solutions to deal with new and emerging challenges.

Many traditional human-led financial crime and compliance solutions are manually intensive, creating issues for firms in terms of customer and employee attrition.

- The better and more efficient the tools that employees must use, the happier – and more loyal – they are likely to be.
- Streamlining the customer journey and experience creates happier customers.

More sophisticated solutions can help financial institutions achieve these goals. Moreover, by leveraging technology and data insights effectively, institutions can strike a balance between protecting themselves and their customers and ensuring they comply with the law. New solutions can enable them to:

- **Identify suspicious activity.** By tracking customer interactions across different touchpoints (onboarding, transactions, account activity, etc.), institutions can identify unusual patterns in or deviations from established behavior that might indicate money laundering, fraud or other illicit activities.
- **Understand risk profiles.** By monitoring customer journeys, firms can build comprehensive customer profiles that incorporate risk factors based on activities, transaction patterns and interactions with the firm, so that higher-risk customers receive closer scrutiny.
- **Proactively investigate.** Continuous monitoring can enable firms to detect suspicious activity in a timelier way, allowing for quicker intervention and investigation before significant losses occur.

These factors are helping to increase and shape the demand for financial crime systems. KYC solutions, for example, are diversifying and expanding. And as the wider marketplace evolves, environmental, social and governance (ESG) factors are becoming more pertinent in the landscape.

Another important dynamic in the market is the shift away from the long-established notion that banks are the sole users of FinCrime and compliance systems and processes. Such solutions are now being implemented and used by a variety of end-user clients, including FinTechs, non-financial banking institutions, insurance companies and payment service providers.

The compliance context

The dynamics of demand are changing on the compliance side too, as firms are compelled to address new and emerging challenges created by a constantly evolving regulatory landscape.

- **Managing third-party risks.** Companies are increasingly responsible for the actions of their suppliers and vendors. Due diligence and ongoing monitoring are crucial to ensure compliance with regulations and avoid reputational damage.
- **Cross-border complexities.** Navigating different legal and regulatory requirements across several countries and/or continents presents a particularly taxing challenge.
- **Data privacy concerns.** Sharing data with suppliers and regulators raises privacy and legal concerns, requiring careful data management practices.

More sophisticated tools are needed

Moreover, to demonstrate that they are complying with regulations and internal policies, firms must keep track of customer interactions and actions. Transparency and accountability are crucial for maintaining regulatory approval and public trust.

Many regulations, particularly in areas such as AML and KYC, require firms to monitor customer activities to track funds and identify suspicious transactions. Again, systems that can monitor customer journeys can help institutions comply and avoid hefty fines.

Notably, for high-risk customers or transactions, firms may require more complex and sophisticated due diligence. Journey monitoring can provide a holistic view of customer behavior, enabling firms to make more informed decisions and implement effective due diligence measures.

Supply-side dynamics: what's shaping solutions

Rising costs, caused by having to comply with regulations and implement systems more widely, are making lower cost of ownership (TCO) and solution affordability increasingly critical for firms.

- **Rising compliance costs.** An ever-evolving regulatory landscape creates a significant compliance burden for institutions, demanding investments in new technologies, processes and personnel. In addition, regulatory bodies are enforcing regulations more stringently, with the attendant risk of fines for non-compliance, making cost-effective solutions even more crucial. Implementing and maintaining data privacy measures adds another layer of complexity and cost.
- **Need for wider adoption.** Smaller institutions and FinTech companies often lack the resources for expensive FinCrime and compliance solutions, hindering their ability to mitigate risks effectively. Making FCC solutions affordable can also widen access to financial services for underserved communities, promoting financial inclusion.

Delivering value

In this context, vendors in the space are delivering value in three ways:

- **Focusing on TCO.** Firms are working with clients or, more broadly, customer segments, to understand the entire value chain in the immediate and longer term. This means incorporating into the 'value equation' aspects such as scalability, cloud economics, customization, output (such as false positive rates) and the resources needed to operationalize and manage the solution set.
- **Looking at gaps beyond the immediate solution set.** Clients and vendors are shifting their focus from the traditional output metrics of core engines (such as false positives), for which gains can often be marginal, toward downstream processes (such as second-line analytics, investigations and suspicious activity report [SAR] filings), which traditionally have been manual and inefficient. Chartis is seeing some exciting innovations in this space, from network analytics used to add contextual information to alerts, to generative AI (GenAI) co-pilots that automate aspects of SAR filing.
- **Packaging solutions to fit the needs of a wider set of markets.** Vendors have realized that there is a need to think and deliver solutions differently for 'adjacent markets', whether these are:
 - Verticals that have not traditionally had the same regulatory requirements, or appetite, for FinCrime solutions.
 - Smaller institutions with different resources and budgets.
 - Institutions from emerging markets where the requirements, and often resources, are unique.

This isn't just about delivering low-cost packaged solutions – in some cases it can be about delivering market expertise or professional services in an accessible way to adjacent markets.

Financial inclusion

One of the key drivers for this focus on adjacent markets is the global drive in the market toward financial inclusion. Policymakers, regulators and financial institutions have traditionally led the push toward financial inclusion, but increasingly vendors are playing a key role in defining and delivering it.

The reasons are not merely commercial, although opening up a vast market beyond core mature markets is an incentive. There is also greater inbound demand from firms that previously would not have considered any form of FinCrime technology.

But there is a key driver in providing tools to detect and prevent FinCrime to institutions that traditionally have not had the same level of access to technology and solutions as their more mature counterparts. This is the realization that to fight FinCrime effectively you need to look at the problem more holistically.

As criminals target segments perceived as being more vulnerable with fewer controls, vendors are working hard to prevent this.

On a practical level, a number of technological advances are helping them deliver effective solutions to emerging segments:

- Cloud hosting, which enables software as a service (SaaS) solutions that are easier and more cost-effective to deploy, scale and upgrade.
- Containerization, which enables modular deployment, development and innovation.
- No-code interfaces, which enable on-the-spot customization without the need for additional resources.
- Measurement and tracking of key operational and performance metrics, which are changing the focus of pricing and licensing.

Nevertheless, as much as tech is enabling and accelerating the shift toward financial inclusion, the most important driver is a culture of collaboration embedded in the industry.

Technology trends and developments

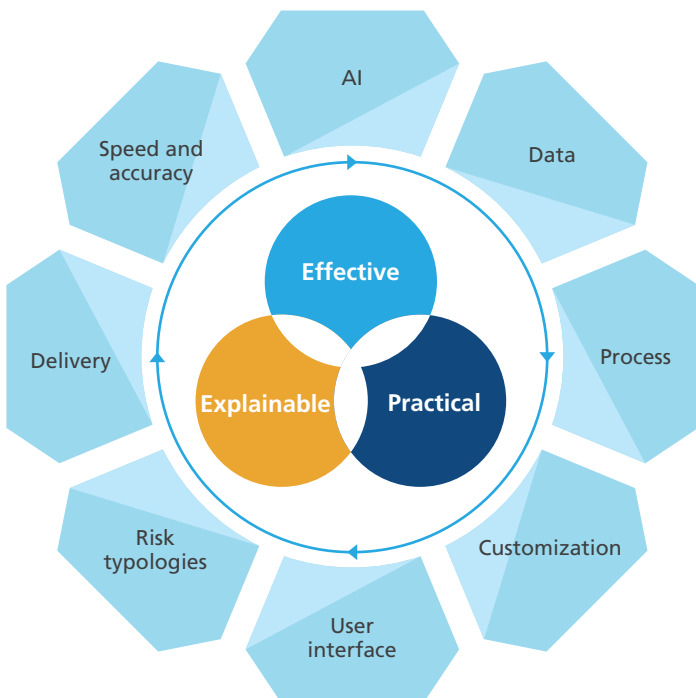
Advances in technology are helping to drive continued evolution in FinCrime and compliance solutions, notably:

- Many solutions can be **purchased and integrated piecemeal**. Clients can save money by starting with one or two modules and expanding as required.
- **Cloud-based solutions**. Compared to traditional on-premise deployments, the cloud offers scalability and cost-efficiency.
- **Open-source technologies**. Open-source tools and platforms provide cost-effective alternatives to proprietary solutions.
- **Artificial intelligence (AI) and machine learning (ML)**. AI- and ML-powered solutions can automate tasks, improve efficiency and reduce manual effort, leading to cost savings.

Focus on AI

As in other areas of risk and compliance technology, Chartis’ conversations with vendors highlight the crucial role that AI will play in financial crime and compliance in 2024. It’s worth noting, however, that while AI and GenAI often take the limelight, the financial crime ecosystem is rich with innovation across a number of vectors, from data to delivery, user interfaces and, of course, AI itself. What is highlighted by the vendors in our ranking, and the ones to watch, is that innovation is by design practical, explainable and impactful (see Figure 5).

Figure 5: The requirements of modern innovation



Source: Chartis Research

There are several key reasons for AI’s growing role, not least its capabilities to enhance efficiency and streamline several important compliance areas, among them KYC, transaction monitoring and sanctions screening.

Enhanced efficiency

AI can improve the efficiency of FinCrime and compliance processes in several important ways: automating repetitive tasks, improving the accuracy and speed of identification, and enabling proactive risk management.

- **Automating manually intensive and repetitive tasks.** AI excels at handling tedious and repetitive tasks (such as transaction monitoring, KYC processes, identifying PEPs and sanctions screening) that are prone to human error. This can free up valuable human resources for more complex and strategic investigations.
- **Improved accuracy and speed.** AI tools can enable firms to identify subtle patterns and anomalies in data that humans may miss, helping companies make faster and more informed decisions about potential risks. Improved accuracy and speed reduce the number of false positives and enable quicker investigations of genuine threats. AI-powered systems can also analyze data and trigger alerts faster, enabling swift investigations of and responses to suspicious activity.
- **Enabling proactive risk management.** AI can analyze data continuously to identify potential risks before they escalate into major issues. This allows institutions to implement measures to mitigate risks before they occur. Firms can also allocate resources more strategically based on their risk appetite.

Areas of improvement: KYC

AI can scrutinize vast amounts of data on customers and transactions, identifying red flags that analysts may miss. Institutions can make more informed decisions during the customer onboarding process and during the ongoing monitoring of their customers, and potentially prevent criminals from entering the system. By analyzing financial history, current customer activity and public records, AI can also uncover hidden connections and suspicious activities linked to certain individuals or entities. Such a comprehensive risk assessment can help firms identify high-risk customers early, allowing for closer monitoring and potentially deterring criminal activity.

Transaction monitoring

Traditional transaction monitoring solutions (TMS) often struggle to keep up with criminals and fraudsters. AI can adapt based on historical data, identifying anomalies and unusual patterns in near-real to real time. Institutions can flag suspicious transactions for further investigation as they occur, potentially preventing financial crimes before they can be committed. AI can also analyze transaction characteristics such as the origin, amount, frequency and recipient of transactions, looking for deviations from established behavior and known thresholds, and identifying patterns associated with known criminal activities. This more proactive approach can reduce the window of opportunity for criminals and mitigate potential losses.

Sanctions screening

Manually screening customers and transactions against constantly growing sanctions lists is a tedious and time-consuming process. AI can automate this task with greater efficiency and accuracy, ensuring that firms comply with regulations and identify potential violations more effectively. AI systems can continuously scan transactions against real-time updates of sanctions lists, including individuals, entities and even specific products or services. This can reduce the risk of accidental involvement with sanctioned entities and minimize the potential for financial penalties for non-compliance.

Responsible implementation

Despite its benefits, AI is a tool, not a magical cure-all. Its effectiveness relies heavily on responsible implementation to ensure that issues such as bias in the training data and transparency and explainability in decision-making are addressed. As AI continues to evolve, ongoing collaboration between financial institutions, technology providers and regulatory bodies is essential to guarantee its ethical and effective use in safeguarding the financial system from criminal activity.

4. Financial Crime and Compliance50 2024 rankings

Rank	Company	Overall score	Rank	Company	Overall score
1	NICE Actimize	82.6	26	Delta Capita	67.0
2	Oracle	81.5	27	Muinmos	66.8
3	SymphonyAI	81.3	28	GBG	66.7
4	LexisNexis Risk Solutions	80.1	29	Kharon	66.5
5	Moody's	79.7	30	Refine Intelligence	66.3
6	Quantexta	78.5	31	DataVisor	65.5
7	LSEG – Risk Intelligence	78.3	32	KYC360	64.7
8	SAS	77.7	33	Xapien	64.5
9	IMTF	77.6	34	Quantifind	64.2
10	Fenergo	75.4	35	AP Solutions IO	63.8
11	ZOLOZ*	74.7	36	SIX Group	63.7
12	ThetaRay	74.6	37	Dixtior	63.5
13	Feedzai	74.1	38	CleverChain	63.3
14	Eastnets	73.6	39	Vneuron	62.5
15	Verafin**	73.3	40	Salv	62.0
16	Ripjar	71.7	41	Neterium	61.2
17	Azentio	71.4	42	smartKYC	60.0
18	ComplyAdvantage	70.9	43	Rozes	58.8
19	HAWK:AI	70.8	44	Prometeia	58.5
20	Appian	70.5	45	Sigma360	58.3
21	Napier	69.8	46	Lynx Tech	57.5
22	Unit21	68.3	47	Crime&tech***	57.2
23	Lucinity	68.2	48	Clari5	56.8
24	IBM	67.5	49	Innovative Systems FinScan	55.3
25	Discai	67.2	50	RZOLUT	54.8

* Part of Ant Group

** A Nasdaq company

*** Spin-off company of Transcrime – Università Cattolica

5. Category winners

Category award	2024 winner
Core technology	
Case management	NICE Actimize
Data enrichment	Quantexa
Data privacy	Muinmos
Emerging data	NominoData
Entity management	Xapien
Know Your Business	CleverChain
Model risk management	SAS
Model testing and development	SAS
Orchestration	Appian
Packaged solution	Dixtior
Perpetual KYC	Moody's
Portfolio monitoring	SIX Group
Real-time performance	AlertSpeed
User interface	Crime&tech
Emerging use cases	
Emerging crime typology detection	Rozes
Enterprise-wide risk management	Arctic Intelligence
Financial inclusion	Manipal Technologies
Policy and control automation	CleverChain
Predicate crime management	ComplyAdvantage
Supply chain risk management	KYC Portal
Trade finance	Cleareye.ai
Vulnerability identification	Cognitive View

Category award	2024 winner
Innovation	
API frameworks	Neterium
Data flow management	norbloc
Data science as a service	Discai
Explainable AI	Ripjar
GenAI initiatives	SymphonyAI
Good behavior modeling	Refine Intelligence
LLM innovation	Ripjar
NLP initiatives	Rozes
Shell company detection	Moody's
Statistical AI	ThetaRay
Risk appetite tuning	DataVisor
Risk typology customization	Kharon
Market-specific capabilities	
Broker-dealer	Muinmos
Global banking	NICE Actimize
Insurance	Azentio
Mid-tier banking	IMTF
Partnership ecosystem	LSEG – Risk Intelligence
Payments	ZOLOZ
Securities	SIX Group
US regional banking	Verafin
Vertical sector flexibility	Vneuron
Wealth management	KYC360

Category award	2024 winner
Regional focus	
Africa	Dixtior
Asia	ZOLOZ
Emerging Europe	Salv
Europe	IMTF
Latin America	Flagright
Middle East	Diligencia
North America	Verafin
Solution	
AML TMS	NICE Actimize
Entity management	Quantexa
Financial crime data management	LSEG – Risk Intelligence
KYC	Fenergo
Sanctions screening	LexisNexis Risk Solutions
Sustainability award	
	Neterium
Workflow and automation	
360-degree customer risk assessment	RZOLUT
Augmented analytics	Quantexa
Integrated workflow	Muinmos
Low-/No-code customization	DataVisor
Reporting and policy automation	RequirementONE
Risk scoring	AlertSpeed
Workflow automation	Lucinity

Category award	2024 winner
Ones to watch	
	<p>AlertSpeed</p> <p>Arctic Intelligence</p> <p>AsiaVerify</p> <p>Cleareye.ai</p> <p>Cognitive View</p> <p>Diligencia</p> <p>Encompass</p> <p>Fincom.co</p> <p>Flagright</p> <p>KYC Portal</p> <p>Manipal Technologies</p> <p>Minerva</p> <p>NominoData</p> <p>norbloc</p> <p>RequirementONE</p> <p>SGR Compliance</p> <p>Tookitaki</p>

6. Appendix A: Research methodology

The FCC50 report assessed almost 300 vendors across the FinCrime core disciplines and narrowed these down to a list of 50.

Vendors were invited to participate in this research through a combination of requests for information (RFIs) and briefings with the Chartis research team.

In addition, we picked a number of award categories that for us reflect the breadth of focus and innovation in this space.

Scoring methodology

The methodology and key scoring criteria for FCC50 follow the Chartis RiskTech100 methodology, a full description of which is available [here](#). However, the FinCrime-specific considerations and focus areas were as follows:

- **Functionality.** The breadth and depth of coverage across the key focus areas of this study, namely sanctions, PEP and adverse media screening, transaction monitoring, KYC, trade-based AML and FinCrime data processes and management.
- **Core technology.** This considers such factors as platform scalability and flexibility, risk typology customization, model quality and validation, model and methodology transparency and explainability, analytics, data management and methodology (proprietary or partner) and user interface (including no-code tuning).
- **Strategy.** This includes strategic clarity, financial performance, growth and other related issues.
- **Customer success.** This looks at excellence in delivering customer value, gauged via case studies, customer and market feedback, as well as other considerations such as financial inclusion, market knowledge and support.
- **Market presence.** This metric considers market presence across verticals (within financial services and beyond) and regions, with an added consideration of emerging markets.
- **Innovation.** This looks at the rate and nature of innovation of a particular vendor. It includes considerations of roadmap and uniqueness of innovation (including patents), with a special focus on AI and GenAI.

7. Further reading



KYC Data and Solutions, 2023: Market Update and Vendor Landscape



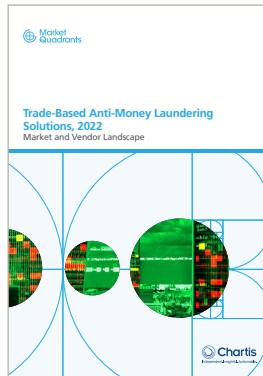
AML Transaction Monitoring Solutions, 2023: Market and Vendor Landscape



FRAML Solutions, 2023: Market and Vendor Landscape



Payment Risk Solutions, 2023: Market and Vendor Landscape



Trade-Based Anti-Money Laundering Solutions, 2022: Market and Vendor Landscape



RiskTech100 2024

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

Contact us

Email: info@chartis-research.com

Phone: +44 20 7316 9964

www.chartis-research.com



Chartis