Vendor Analysis

Vendor Analysis: SAS

AML Transaction Monitoring Solutions, 2023

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.

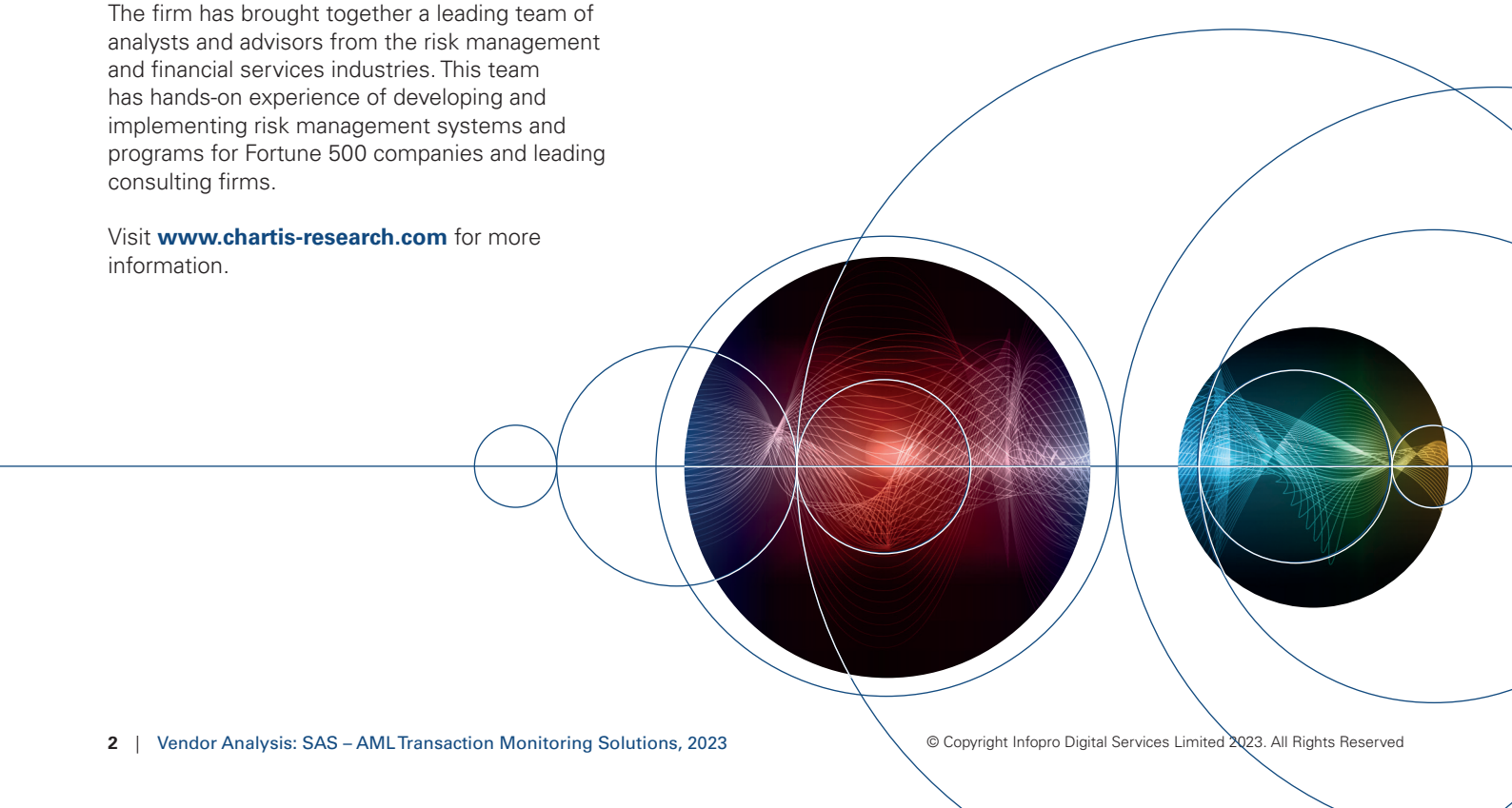


Table of contents

List of figures and tables

1. Report context

This Vendor Analysis is based on the Chartis quadrant report *AML Transaction Monitoring Solutions, 2023: Market and Vendor Landscape* (published in November 2023). This section summarizes the key theses in that report; subsequent sections take a detailed look at SAS' quadrant positioning and scoring, and Chartis' underlying opinion and analysis.

Key thesis

Key dynamics in the landscape

Until recently, the AML software space typically supported compliance-focused FinCrime strategies

Historically, providers of anti-money laundering (AML) transaction monitoring systems have considered themselves to be agnostic to the underlying risk strategies of their financial institution clients, believing they do not constitute a core concern. Instead, they've seen their role as providing a way for banks to achieve a risk-based approach to money laundering and the detection of other financial crimes. Generally, banks have focused on compliance-centric approaches to detecting financial crime, concentrating on capturing classic AML typologies to stay compliant with regulations and engaging in defensive filings of suspicious activity reports (SARs) to protect themselves from further exposure to regulatory risk.

Tackling financial crime is shifting from a compliance requirement to a key operational concern

In recent years, banks have recognized that financial crime risk can manifest in ways other than compliance and regulatory risk. Banks are increasingly treating anti-financial crime strategies as crucial initiatives within their operational risk programs, to tackle the following challenges:

- Counterparty risk associated with facilitating financial crime.
- Reputational risk associated with money laundering scandals.
- Emerging environmental, social and governance (ESG) investment risk associated with the ethical impacts of financial crime.
- More traditional financial losses from fraud and asset seizures.

Intelligent automation and integration can fuel more effective AML detection strategies

Recent innovations in advanced analytics are enabling banks and other firms to reimagine how they identify AML risks in their customers' activity. Emerging solution providers are solving an array of AML detection challenges by augmenting the various steps of the AML risk management lifecycle with analytics-enabled risk intelligence. Technologists are increasingly infusing intelligence across the AML risk management lifecycle, from risk assessment at the front end, customer due diligence (CDD) and AML transaction monitoring to reporting, controls testing and risk-control alignment. This is transforming what banks can expect from an end-to-end AML transaction monitoring system. The technology to boost the effectiveness of AML systems is arriving and it is now up to banks to decide whether – or how – to use it.

Core systems and component solutions are converging, changing the dynamics of the tech stack

Increasingly, Chartis is seeing core system vendors build or buy analytics component solutions and shift their approach from linear software products to a more modular and open-platform architecture. 'Platform' in this sense refers to how vendors enable the integration of additional data sources and models within their solutions' core risk engines. Component providers are fundamentally unprepared for the convergence of core systems with additional components and must be very specific about not just who their potential customer is but also who their target partners are. While the first wave of AML transaction monitoring partners targeted analytics use cases, newer market entrants are trying several unique angles, including customer outreach tools, which go beyond pure-play analytics.

Regulators are slow to adapt to intelligence and analytics-enabled model opportunities

Many organizations are still concentrating on augmenting analytics. While this is operationally effective, it can miss certain tail risks that can

lead to program failure and regulatory penalties. Regulators have also been slow to respond to these changes – despite the ineffectiveness of the current system, minimal penalties have been granted in recent years. However, on the heels of Financial Action Task Force (FATF) guidance endorsing the application of digital technologies and regulatory sandboxes empowering firms to test new models, it appears that regulators are becoming more comfortable with advanced analytics techniques.

Financial institutions should be proactive in preparing for the convergence of risk assessment/intelligence and core transaction monitoring systems. They should evaluate their current AML transaction monitoring solutions and consider investing in new technologies that can help them identify and mitigate risk more effectively. Regulators should also take a more proactive approach to AML enforcement by increasing penalties for AML violations and enforcing compliance in such niche areas as trade-based AML (TBAML). By working together, financial institutions, vendors and regulators can create a more effective AML system.

Demand-side takeaways

Less enforcement, more criminality

AML enforcement is currently in a relative lull – minimal penalties have been imposed for AML violations in recent months. This is despite a continued increase in criminality, including fraud, scams and white-collar crime. According to the **Federal Trade Commission (FTC)**, consumers reported losing nearly $8.8 billion to fraud in 2022, an increase of more than 30% on the previous year. On a related note, the Office of the Comptroller of the Currency (OCC), the Financial Crimes Enforcement Network (FinCEN), the Federal Deposit Insurance Corporation (FDIC) and the Federal Reserve **completed 19 enforcement actions in 2022** following instances of AML. This was nearly double the number in 2021 (11), but still much less than the 40 recorded in 2020. Global transaction flows are increasing, making it more difficult to detect money laundering. In addition, the ongoing concentration of global wealth into family offices and high-net-worth individuals (HNWIs) makes it easier for criminals to disguise their activities. Family offices and HNWIs often have complex financial structures that can be used to conceal money laundering. As of 2021, **annual losses from white-collar crime** were estimated to be between $426 billion and $1.7 trillion – this wide range is due to the lack of prosecutions (and the associated gap in crime statistics that results). It is believed that as many as 90% of white-collar crimes **are not reported**.

Complex asset classes, such as trade finance and alternatives, are also being used to launder money. Real estate is a popular vehicle for money launderers, as it is a relatively illiquid asset, making it difficult for law enforcement to track and seize the proceeds of a crime. Criminals commonly use cash to purchase properties and introduce illicit funds into the financial system, as the source of funds is difficult to trace. Shell companies and straw buyers[1] are also commonly used in real estate to conceal identities and sources of funds. Trade finance is a complex global industry that often involves the movement of goods and funds across borders. This complexity makes trade finance a popular avenue for money launderers, as it helps to obscure the true purpose of a financial transaction by masking money laundering under the veneer of international trade.

Although detection rates seem lower for complex money laundering techniques, simpler methods may make up the majority of money laundering efforts. 'Smurfing'[2] and through-account fraud, for example, are becoming common in retail banking, and recent research among vendors indicates that as many as 0.3% of retail bank accounts in the US **may be being used** for money mule services.

Know Your Customer (KYC) continues to play an important role in detecting money laundering. It is now being supplemented by enhanced due diligence (EDD) processes and customer feedback. For EDD, firms collect additional information about customers who are considered high-risk, such as politically exposed persons (PEPs) or those from high-risk countries. Customer feedback can also be used to identify suspicious activity, such as unusual transactions or changes in customer behavior. Increasingly digital transaction signals such as these are being fed directly into transaction monitoring systems and the risk detection algorithms that sit within them.

Transaction monitoring systems – a choice of approaches

Fundamental transaction monitoring is the traditional approach. It focuses on identifying suspicious activity by analyzing financial

[1] *Someone who makes a purchase on behalf of someone else, possibly for fraudulent ends.*
[2] *Breaking large amounts of money into smaller quantities for laundering, to avoid detection.*

transactions against a set of predefined rules. These rules are typically based on historical data, regulatory requirements and expert knowledge, and they may flag transactions that are considered high-risk. These might include large cash withdrawals, frequent transfers to overseas accounts or transactions that are inconsistent with a customer's normal spending patterns.

Quantitative transaction monitoring is a more data-driven approach that uses machine learning (ML) and artificial intelligence (AI) to identify suspicious activity. Quantitative models are trained on large datasets of historical financial data, and they learn to identify patterns that are indicative of money laundering or other financial crime. Quantitative models can be more effective than fundamental rules-based systems at detecting new and emerging types of fraud, and they can also be more efficient at processing large volumes of transactions. Within this group, ML-driven approaches leverage feedback and iteration to improve over time, whereas deep learning (DL) systems are developed over time to become more sophisticated at pattern recognition.

The best approach to transaction monitoring for a particular financial institution depends on its specific needs. Institutions with limited resources may find fundamental transaction monitoring a good option. However, institutions that are processing large volumes of transactions or that are concerned about new and emerging types of fraud may want to consider using a quantitative approach. In reality, most financial institutions are using a hybrid approach to transaction monitoring, combining elements of both methods. This approach provides the best of both worlds, offering the flexibility of a fundamental rules-based system and the accuracy and efficiency of a quantitative one.

Supply-side takeaways

The vendor landscape for transaction monitoring solutions is evolving: new vendors are emerging and established vendors are expanding their offerings. While the market is dominated by a few large players, several smaller vendors are offering innovative solutions. These firms provide a range of transaction monitoring solutions, from on-premises to cloud-based, simple to complex, and component to enterprise offerings.

Core system vendors have traditionally been slow to innovate in the AML space – until recently. This is the result of several factors, including the complexity of core systems, the need to maintain backward compatibility and the cost of innovation. Numerous component players are offering functionality to plug the gaps in core systems' AML capabilities – these firms are typically more innovative than core system vendors.

In recent years, however, we have begun to see the major incumbents invest heavily in advanced analytics capabilities. Some firms have invested extensively in ML, while others are developing their DL capabilities. When it comes to ML, we are seeing a few firms engage in 'co-opetition' (it is unclear whether these solutions are competitors or complements):

- **Generalist ML studios**. These products sit at the intersection of closed and open source, allowing firms to take advantage of what data science libraries have to offer, while also building on top of IP provided by companies.

- **Pre-built models**. Many firms offer pre-packaged ML models that address a specific requirement within a workflow, such as classifying transaction activity or other forms of anomaly detection. Typically, these models are partly 'black box' in nature, as they are not fully exposed to the end user. While this is a classic strategy of core providers, some component solution vendors also compete in this space.

- **Models as a service**. This is a relatively new concept within AML. Essentially, rather than delivering a completely plug-and-play model, some enterprising vendors are providing the shell of a library of pre-built models that can be rapidly customized to capture the intersection of risks with operational complexity. For example, normal customer behavior may differ by segment or geography; typically, this last-mile model development is taken on by a team of data scientists at a bank. Perhaps a better term for the concept is 'Modeling as a service,' as the outcome for customers is exactly that: a rapid mechanism for translating the nuances of a firm's risk profile into a set of customized detection algorithms.

The most successful players are those that offer ML and DL anomaly detection capabilities. ML and DL anomaly detection is a powerful tool that can be used to identify suspicious transactions that would be difficult to detect using traditional methods. ML and DL are used in a variety of ways within transaction monitoring to improve its accuracy and efficiency, including anomaly detection, transaction clustering, entity resolution and/or behavioral analytics.

2. Quadrant context

Introducing the Chartis RiskTech Quadrant®

This section of the report contains:

- The Chartis RiskTech Quadrant® for AML transaction monitoring solutions, 2023.
- An examination of SAS' 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?

Chartis' 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 transaction 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 riskf technology marketplace. It considers 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 Quadrant® and FinTech Quadrant™ 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 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' 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 transaction monitoring solutions, 2023

Figure 1 illustrates Chartis' view of the vendor landscape for AML transaction monitoring solutions, highlighting SAS' position.

Quadrant dynamics

Vendor positioning in context – completeness of offering

SAS' transaction monitoring solution provides strong capabilities in almost every area. The vendor received a high rating for its data and systems integration capabilities, which are powered by multiple offerings. Notable among these is SAS' Financial Crime Decisioning, an enterprise fraud capability designed for financial institutions and non-banking financial firms that aim to mitigate risk across the entire customer lifecycle. Embedded customer lifecycle event monitoring is designed to accept financial and non-financial transactions from across channels and products. This is complemented by internal and external data; real-time enrichment is also performed

Figure 1: RiskTech Quadrant® for AML transaction monitoring solutions, 2023

Source: Chartis Research

to support optimal financial crime risk management. This capability, in combination with SAS' patented Signature-based approach to profiling, captures entities and their data across multiple sources, analyzing it for patterns and inconsistencies every time a transaction occurs. It is accurate up to the millisecond.

SAS also received a high rating for its expansive risk typology modeling, which enables firms to build a compliant transaction monitoring program with relative ease. With wide coverage across the financial crime spectrum, from product and channel risk to high-risk entities, these libraries begin with scenario templates, based on industry trends, that firms can use on implementation. Risk typologies can then be enhanced and adjusted to meet all compliance requirements.

Analytical modeling and model quality/validation are two other capabilities offered by SAS' Financial Crime Decisioning solution. The solution allows end users to visually explore and evaluate data for further analysis using k-means clustering, scatter plots and detailed summary statistics. The offering simplifies the creation, analysis and validation of models using advanced ML and AI algorithms. End users can identify and design typologies to target specific groups or segments, and numerous 'what-if' scenarios and analyses are available.

SAS features post-alert scoring and segmentation out of the box, allowing end users to integrate statistical modeling into every process related to financial crime detection. The SAS solution

provides a range of model validation and performance monitoring capabilities, such as:

- Model decay.
- Automated retraining of models when thresholds are exceeded.
- Governance via a centralized model repository with templates and version control.
- Lineage for SAS and open-source models.

Chartis' rating for SAS Financial Crime Decisioning's workflow automation was particularly strong, reflecting the company's innovative AI and ML algorithms. The solution's key technology components allow end users to investigate and disposition alerts and events, suppress alerts for a chosen period, re-open closed alerts and initiate cases for deeper investigation. Multiple alerting events are consolidated within a single work package, giving users a comprehensive view of related intelligence, including prior cases and regulatory filings, customer risk ratings and fraud activity.

End users can link related customers, alerts, cases or virtually any object within the system. All of this is provided via real-time network and entity generation processes to enable firms to automatically build network diagrams, resolve real-world entities and uncover hidden relationships based on the latest data. Compliance managers can prioritize analyst activities, monitor productivity and effectiveness, and adapt surveillance strategies to new and emerging patterns.

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

Vendor positioning in context – market potential

SAS has established itself as a leader in transaction monitoring services. The company's AML transaction monitoring offerings combine regulatory compliance with human-led and tech-powered services – a breadth of capabilities reflected in the vendor's category leader position in the quadrant.

Table 1: Completeness of offering – SAS (AML transaction monitoring solutions, 2023)

Completeness of offering criterion	Coverage
Data and systems integrations	High
Risk typology modeling	High
Analytical modeling	High
Model quality and validation	High
Workflow automation	High
Solution packaging and deployment	Medium

Source: Chartis Research

Table 2: Market potential – SAS (AML transaction monitoring solutions, 2023)

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

Source: Chartis Research

Notably, the robust ratings for customer satisfaction and market penetration reflect the company's expansive, global client base, which covers a vast array of financial institutions, including, but not limited to, banks, credit unions and FinTechs.

SAS' strong ratings for growth strategy and financials also reflect continued demand for its services. To keep up with expanding demand, SAS continues to widen its client base and areas of focus, alongside its already extensive workforce.

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

3. Vendor context

Overview of relevant solutions/ capabilities

Table 3 provides a summary of the vendor and its solutions.

SAS' fraud and financial crime solutions are built on a common technology architecture that can be deployed to address both fraud risks and money laundering/terrorist financing risks (see Figure 2).

SAS Anti-Money Laundering software includes intellectual property for mapping transaction, account and entity dimensions in support of both fundamental and quantitative transaction monitoring strategies. Increasingly, clients are using data orchestration to enrich monitoring or investigative processes with third-party data (such as the risk rating of virtual asset service providers). As part of the SAS Viya 4 cloud-native architecture, the solution is designed to optimize and govern the use of open-source programming languages (R, Python, Lua, etc.) for clients that wish to augment their existing processes with AI and ML.

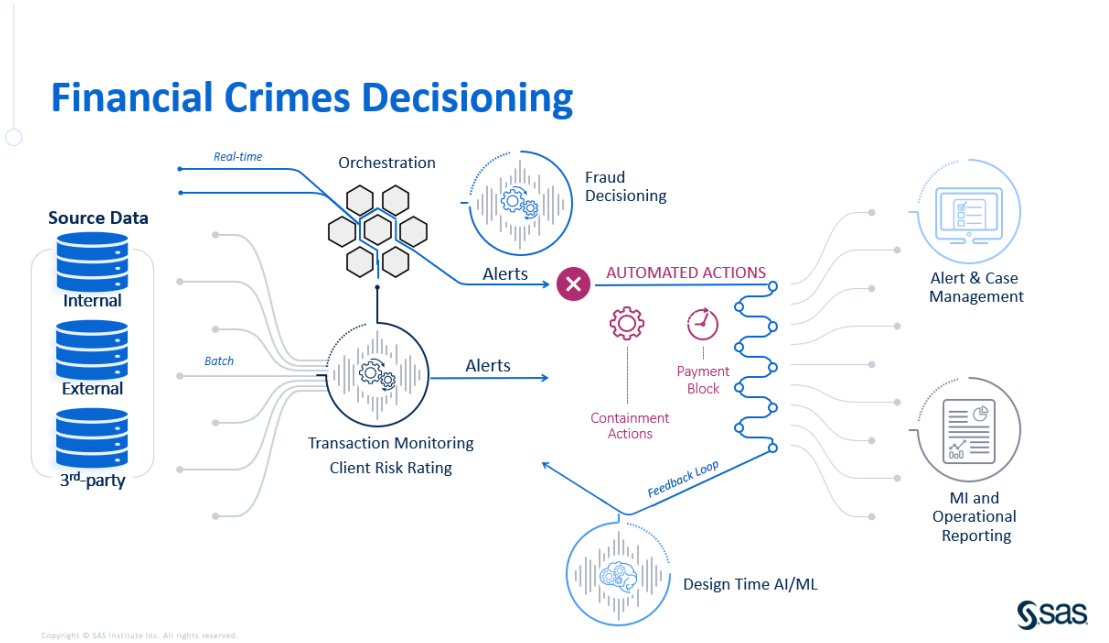
SAS Anti-Money Laundering features a highly scalable behavioral monitoring system with out-of-the-box (OOTB) scenarios for cash, wire, correspondent banking and anomaly detection. The system has been enhanced to support behavioral segmentation strategies and advanced alert scoring. Many clients use advanced scoring logic to automate the triage of alerts to investigation. SAS' new case management tool can be configured to support a wide range of financial crime investigations. The tool supports elastic search and provides dynamic link analysis as a standard OOTB feature.

Table 3: SAS – company information

Company	SAS
Headquarters	Cary, NC, US
Other offices	SAS has offices in 56 countries worldwide.
Description	SAS, one of the largest privately held software companies in the world, provides AI and advanced analytics tools to customers globally, including 91 of the top 100 companies in the Fortune 500. SAS has evolved its fraud and financial crime solutions since the introduction of SAS Anti-Money Laundering software in 2002. SAS' clients for these offerings range from global systemically important banks (G-SIBs) that rely on SAS solutions for real-time fraud interdiction, to small and medium-sized institutions that use SAS' software to comply with money laundering regulations. Solutions are built on the cloud-native SAS Decisioning Architecture.
Solution	SAS' fraud and financial crime solutions are built on the SAS Decisioning Architecture, which provides a consistent technology stack that has been refactored for cloud-native deployment. The Decisioning Architecture is built on the SAS Orchestration Command Line Interface (CLI) and industry-standard application programming interfaces (APIs) that allow data to be ingested into its transaction monitoring environment. The monitoring engine supports Boolean and advanced ML strategies that can be deployed in real time, near-real time or batch. The alert and case management tools are based on open-source business process management (BPM) standards, and enable firms to automate triage decisions as necessary. To support closed-loop self-learning and reporting, the Decisioning Architecture captures outcomes for reporting and the dynamic refresh of signatures.

Source: SAS

Figure 2: SAS' fraud and financial crime architecture



Source: SAS

Beginning with the SAS Viya 4 release, SAS Customer Due Diligence will be included with SAS Anti-Money Laundering software so that firms can have more tightly integrated scoring between KYC measures and actual behavior. The event-based triggering of EDD reviews enables firms to deploy perpetual KYC.

Once events have triggered a review or an investigation, work items are persisted in SAS' alert and case management tool. Screens have been configured for such specific types of activities as fraud alert reviews, AML investigations, EDD or manual case entries. Clients can simply modify screens and workflow via a drag and drop administrative interface.

Many SAS clients leverage the 'design time' financial crime analytics capabilities found in SAS' ML tools. SAS supports the entire AI lifecycle, from data acquisition to champion-challenger design, and the testing of strategies to deployment. SAS' natural language processing (NLP) methods have been effective in detecting trade-based money laundering risks hidden in text in unstructured data (such as letters of credit, goods descriptions, etc.).

Vendor leading practices

SAS' expertise in AI/ML comes from deploying fraud and financial crime solutions to global clients for more than 20 years. The company has a tremendous amount of institutional knowledge that varies across disciplines from fraud to compliance. SAS' risk, fraud and compliance solutions team understands not only the business requirements for risk management, but also the steps required to satisfy model governance concerns that are top of mind during the deployment of AI.

With its strength in analytics, SAS can help clients adopt more innovative strategies for managing AML compliance risks. The vendor's subject-matter experts support clients through:

- Periodic 'health checks' to assess the efficacy of monitoring programs.
- Proven techniques for assisting clients on their 'NextGen' journey to adopt anomaly detection, behavioral segmentation, process automation and ML-based detection strategies.
- Recommended strategies for tagging investigation outcomes to inform tuning/optimization.

- Advanced ML methods for entity resolution.
- ML models for client risk rating.
- API strategies for enriching and automating the use of third-party data to reduce manual processes.

SAS has collaborated with several G-SIBs on AML innovations. During the next 12 to 18 months, the company expects to standardize AI/ML capabilities as OOTB offerings. This should enable small and medium-sized banks to consume more quantitative monitoring practices faster and more easily.

Through the work of its Data Ethics Practice and its collaboration with government agencies on regulatory controls, SAS aims to be a trusted provider of AI technologies. Given the company's experience in model risk management technologies, it will continue to leverage AI and ML to improve the effectiveness of transaction monitoring disciplines. It will also use generative AI to make it easier for clients to document, explain and defend next-generation AML.

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 Quadrant® 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 sectors, 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 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 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 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.

Briefing process

We conduct face-to-face and/or web-based briefings with each vendor.[3] During these sessions, Chartis experts ask in-depth, challenging questions to establish the real strengths and weaknesses of each vendor. Vendors provide 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 uses other third-party sources of data, such as conferences, academic and regulatory studies, and publicly 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 used for AML Transaction Monitoring Solutions, 2023 are shown in Table 4.

Completeness of offering

- **Depth of functionality**. The level of sophistication and number 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 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 can vary for each subject area, but special attention is given to functionality covering regulatory requirements, multiple risk classes, multiple asset classes,

[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.*

Table 4: Evaluation criteria for Chartis' AML transaction monitoring solutions (2023) report

Completeness of offering	Market potential
• Data and systems integrations	• Customer satisfaction
• Risk typology modeling	• Market penetration
• Analytical modeling	• Growth strategy
• Model quality and validation	• Financials
• Workflow automation	
• Solution packaging and deployment	

Source: Chartis Research

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 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 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 category and, by extension, to 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.

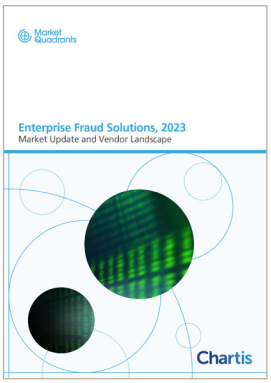
Category leaders

- 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.

Further reading

AML Transaction Monitoring Solutions, 2023: Market and Vendor Landscape

FRAML Solutions, 2023: Market and Vendor Landscape



Enterprise Fraud Solutions, 2023: Market Update and Vendor Landscape

KYC Data and Solutions, 2023: Market Update 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**