Vendor Analysis

Vendor Analysis: SAS

Enterprise Fraud 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.

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

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.

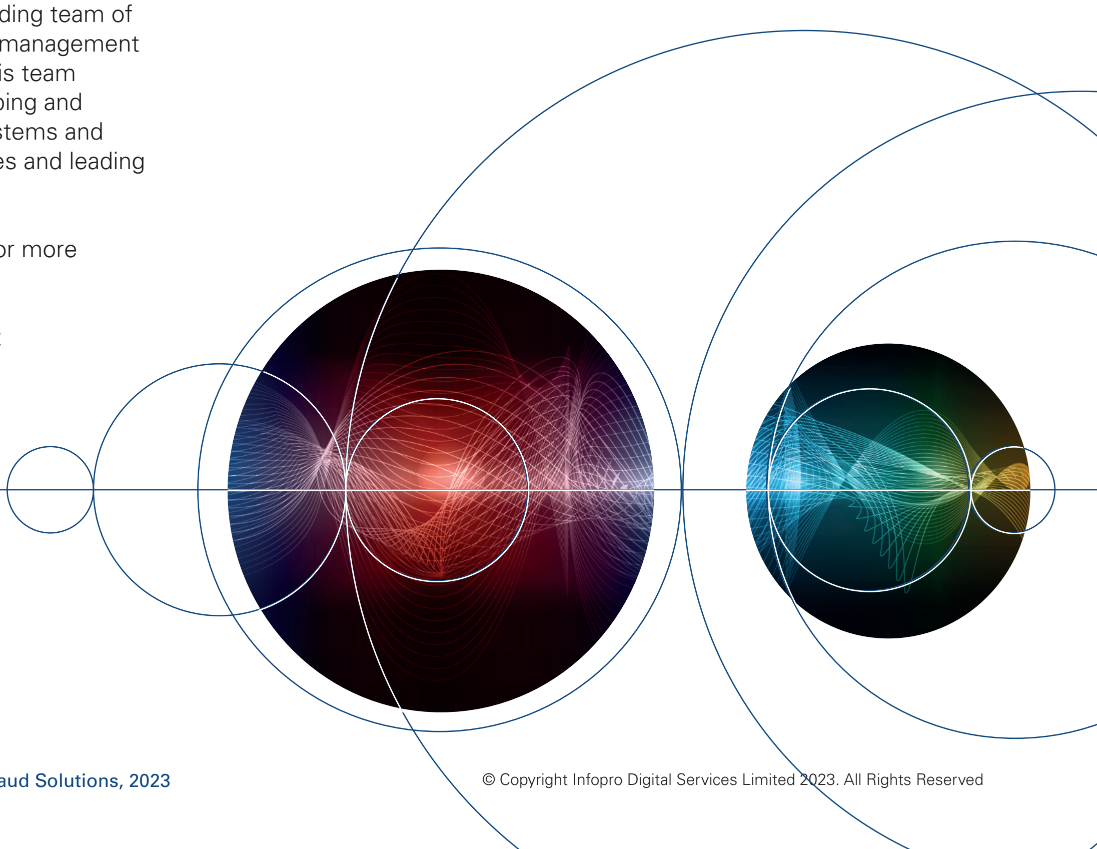


Table of contents

List of figures and tables

1. Report context

This Vendor Analysis is based on the Chartis quadrant report *Enterprise Fraud Solutions, 2023: Market Update and Vendor Landscape* (published in May 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

The latest iteration of our ongoing research into enterprise fraud solutions covers several key themes in the market, notably around model risk, use of the cloud, the growth in artificial intelligence (AI), and the increasing speed of payment systems and services.

In a solutions market still mostly driven by the large, complex frauds occurring in investment banking, financial institutions and vendors are developing their technological capabilities to address an ever-evolving landscape of fraud. As regulators focus in on the importance of model risk management, firms and vendors are having to integrate, test and explain more complex models, and deal with challenges around the vast quantities of data they must now analyze and interpret.

The increasing 'commodification' of AI, in the form of consumer-friendly apps such as ChatGPT, could trigger a new wave of fraud as criminals adopt these powerful (albeit costly and hard to maintain) tools. Meanwhile, the increasing speed with which companies and individuals can carry out payments is creating more opportunities for criminals to act faster than some fraud systems can handle.

Finally, many firms are beginning to see past the hype surrounding the all-pervasive cloud, realizing that its undoubted benefits – scalability, flexibility and security – must be balanced with their own specific requirements, many of which may not align with what the cloud has to offer.

These factors are generating several themes in the vendor landscape, as technology providers lean into the dynamics of specificity, scale and connectivity, while also focusing more attention on model agility, analytics and multichannel capabilities.

Demand-side takeaways

In the latest update to our research, we have identified several key themes:

- **The continued role of investment banking in driving the solutions market**. For vendors that supply anti-fraud solutions, the differentiation between fraud in retail banking and that in investment banking continues to be a significant market dynamic. Although many vendor firms have gained a considerable foothold in the retail marketplace, the anti-fraud solutions market tends to lean more toward the investment side of the equation, largely because of the size of transactions, the complexity of financial products, and counterparty risk.

- **The growing importance of model risk management (MRM) and validation, and the increasing complexity of the data required**. Model validation and testing are crucial to ensure that models are performing as intended. MRM is also essential to ensure that models are used appropriately and that any potential risks are identified and mitigated. Validating and testing anti-fraud models can be difficult, however, because there may be a limited number of instances of fraud to test against, and the models may not detect all fraud types.

- **The commodification of AI and its potential to trigger new types of fraud**. When it comes to a discussion of data processing, the rise of ChatGPT and large language models (LLMs) has been difficult to ignore. Financial institutions and the wider technology industry are looking for ways to capitalize on the capabilities demonstrated by foundation models in general, and LLMs specifically. These models have particular strengths (they return legible, context-sensitive written information from a large corpus of data) and weaknesses (they predict rather than retrieve information, so are prone to inaccuracies or 'hallucinations').

- **The growing popularity and speed of payments**. Faster payments continue to push up transaction speeds. Notably, FedNow, the payment service launched by the US Federal Reserve in 2022, aims to offer a fast and secure payment option to consumers and businesses in the US, with 24/7 availability. The US has been something of a laggard in enabling faster payments, so FedNow can be seen as a milestone in the broader market trend of 'faster, everywhere'. This creates two broader trends for anti-fraud systems: reduced transaction-processing times and increased transaction volumes.

- **The cloud equation – how firms are balancing the benefits with their specific requirements**. Flexibility continues to be a watchword for anti-fraud solutions – and, as such, cloud deployments of these systems have been increasingly important. However, this is one trend that is no longer fixed, and there is, if not some pushback, at least a lessening of the cloud hype. Some institutions have found that their legacy systems do not operate well with cloud application programming interfaces (APIs) and containerizations, and that the cost can be higher than expected. And major cloud selling points (such as scalability) may not be as relevant to firms that have relatively stable transaction volumes.

Supply-side takeaways

From the perspective of technology, leading vendors are focusing on the *agility of models*, to enable quick modifications and updates in response to evolving fraud patterns. This allows financial institutions to stay ahead of emerging fraud threats and respond quickly to new challenges. And by providing more flexible and adaptable model-management capabilities, vendors can differentiate themselves in the marketplace and win market share.

'Self-service' in analytics is increasingly important, in that it enables institutions to tailor their fraud detection and prevention strategies to their specific needs and requirements, and obviates the need to rely solely on pre-packaged solutions. This approach can also be more cost-effective and efficient for institutions, as they can use their own in-house expertise and resources.

Our research also reveals that *connectivity* and the ability to connect to third parties through APIs are common capabilities among vendors, enabling solutions to integrate with existing systems and workflows. This provides a standardized way for third-party applications to access data and functionality from anti-fraud solutions. The approach also lends itself to rapid deployment of new features and updates, and means that firms can scale up or down as required.

Vendors using APIs were seen to be offering their clients greater transparency and control, enabling them to monitor and manage their use of solutions in real time. This is particularly prevalent among Tier 1 organizations with complex IT environments.

2. Quadrant context

Introducing the Chartis RiskTech Quadrant®

This section of the report contains:

- The Chartis RiskTech Quadrant® for enterprise fraud 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?

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 enterprise fraud 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 enterprise fraud solutions, 2023

Figure 1 illustrates Chartis' view of the enterprise fraud solutions vendor landscape, highlighting SAS' position.

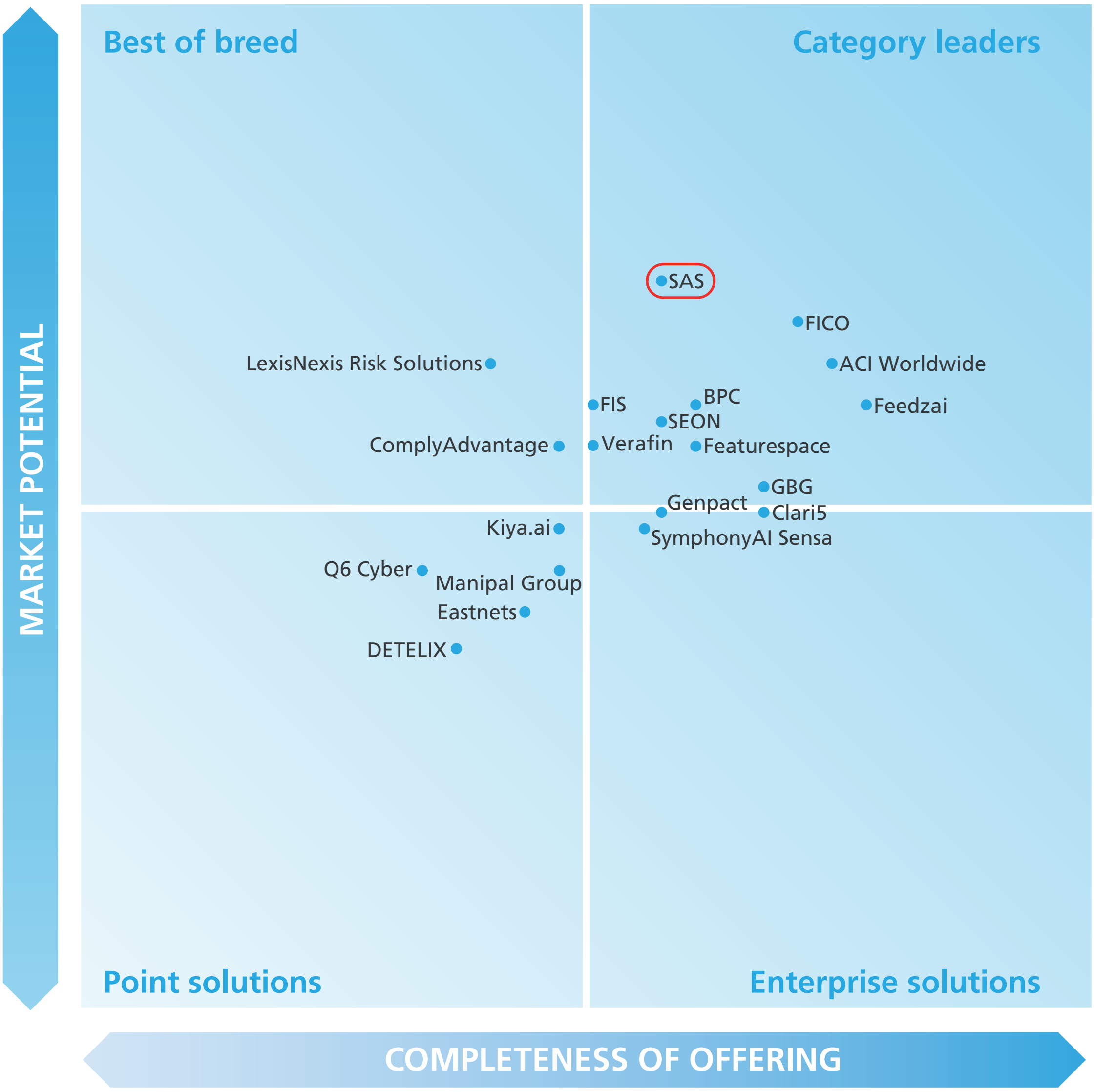
Quadrant dynamics

General quadrant takeaways

A trend in the anti-fraud landscape noted in the Chartis report *Financial Crime Risk Management Systems: Enterprise Fraud; Market Update and Vendor Landscape, 2021* was *specificity*, across verticals and geographies. While regional specificity remains a key feature of the anti-fraud landscape, the market has also been increasingly characterized by *scale*.

The vendors in the enterprise fraud quadrant have almost universally been those that are able to post strong growth with replicable, profitable business models. As such, a broad solution capability, robust

Figure 1: RiskTech Quadrant® for enterprise fraud solutions, 2023



Source: Chartis Research

support and service capabilities and a strong regional footprint are increasingly seen as 'table stakes' within the market.

Vendor positioning in context – completeness of offering

SAS' enterprise fraud solution provides strong capabilities in almost every area. The vendor received a high rating for its behavioral monitoring capabilities, provided via multiple solutions, notably SAS Fraud Management. An end-to-end fraud detection and prevention solution, this offering enables enterprise-wide monitoring from a single platform. The solution's embedded machine learning (ML) capabilities are programmed to detect and adapt to changing behavioral patterns, resulting in more effective, versatile models. In addition, SAS' patented Signature-based approach to profiling captures customer behavior and data from multiple sources, analyzing it for patterns and inconsistencies every time a transaction occurs. Dynamic updates to these profiles occur in real time for every transaction.

SAS received a high rating for its libraries of pre-packaged fraud rules and models, which can enable firms to build a compliance program. With wide coverage across the fraud spectrum, from account to payments fraud, these libraries begin with 'starter rules' that are based on industry trends, and which firms can use on implementation. Fraud rules can then be further enhanced and adjusted to meet all compliance needs.

Case management and workflow are two other capabilities offered by SAS' Fraud Management solution. The offering simplifies data integration, enabling firms to combine all internal, external and third-party data to create better predictive models to suit a company's particular compliance needs. Combining this data on a single technology platform gives firms the flexibility to scale as they change and respond to new fraud trends. As workflows improve and the technology generates fewer false positives, firms can provide a better customer experience while detecting more instances of fraud.

Chartis' rating for SAS Fraud Management's transactional monitoring was particularly strong, reflecting the company's behavioral monitoring capabilities. The solution's key technology components allow users to spot anomalies easily for every customer. In-memory processing delivers high throughput and low-latency response times – even in high-volume environments – enabling firms to score every transaction in real time.

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

Vendor positioning in context – market potential

The breadth of capabilities offered by the SAS Fraud Management solution – which combines regulatory and market insight with human- and tech-led services – contributed to SAS' category leader position in the quadrant. Notably, the strong ratings for customer satisfaction and market penetration reflect the company's large client base, which comprises a variety of firms, including – among others – financial services companies and technology organizations.

SAS' robust ratings for growth strategy and financials reflect growing global demand for its services, which has helped to boost company revenues by more than 20%. To keep up with this expanding demand, SAS has widened its client base and areas of focus, and has taken advantage of its extensive global workforce.

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

Table 1: Completeness of offering – SAS (enterprise fraud solutions, 2023)

Completeness of offering criterion	Coverage
Advanced/proprietary fraud-detection techniques	Medium
Behavioral monitoring	High
Libraries of pre-packaged fraud rules	High
Case management and workflow	High
Transaction monitoring	High
Identity management capabilities (e.g., device ID, etc.)	Medium

Source: Chartis Research

Table 2: Market potential – SAS (enterprise fraud solutions, 2023)

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

Source: Chartis Research

3. Vendor context

Overview of relevant solutions/ capabilities

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

SAS is a leader in business analytics software and services, and the largest independent vendor in the business intelligence market. The company's solutions enable customers at more than 80,000 sites to make decisions faster and improve their performance. Founded in 1976, SAS focuses on analytics, data science and ML; over the decades, this scope has grown to cover specializations across multiple industries.

SAS' fraud and financial crime solutions (F&FC) are used by 300 financial institutions globally, many of which use SAS for both fraud and compliance. In addition, two-thirds of global systemically important banks (G-SIBs) use SAS for F&FC solutions, contributing to 23% growth in total revenue for these offerings in 2021.

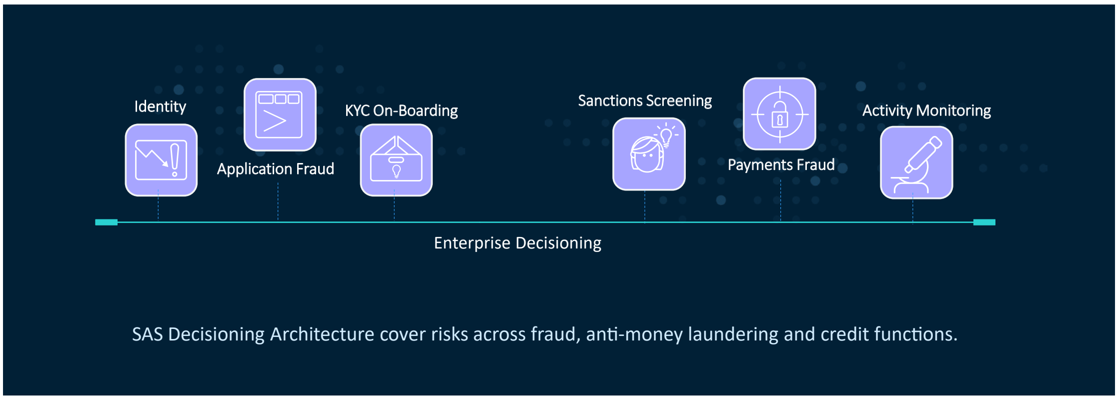
SAS' fraud and security intelligence solutions take a unified approach to fraud, compliance and security, delivering an essential layer of protection backed by domain expertise and advanced analytics.

Table 3: SAS – company information

Company	SAS
Headquarters	Cary, NC
Other offices	SAS has offices in 56 countries worldwide
Description	SAS, one of the largest privately held software companies in the world, is a leading provider of AI and advanced analytics tools. Used by 91 of the top 100 companies in the global Fortune 500, SAS provides software and services to customers around the world. SAS' Enterprise Fraud solution offers enterprise decisioning capabilities that span all areas of risk and marketing intelligence. The solution optimizes common capabilities, beginning with intelligent data orchestration and enrichment, and mapped to a configurable data layer. Model development and decision authoring are seamlessly operationalized into a multi-function decisioning engine. Operational activities, including customer self-service alerts, are complemented by manual investigations that are performed through flexible alert triage and a case management interface.
Solution	A modular system, SAS' enterprise fraud solution offers tightly integrated components with an end-to-end risk capability. SAS ensures that financial institutions can detect, identify, prevent and validate threats from external and internal sources. The advanced analytics that SAS applies through its ML capabilities continue to be core to the solution, allowing customers to keep pace with evolving challenges in fraud and financial crime. Underpinned by a cloud-native platform, the solution is designed to accommodate the increasing data volumes firms require to consume remote-channel data at high throughput and low latency.

Source: SAS

Figure 2: The SAS decisioning architecture



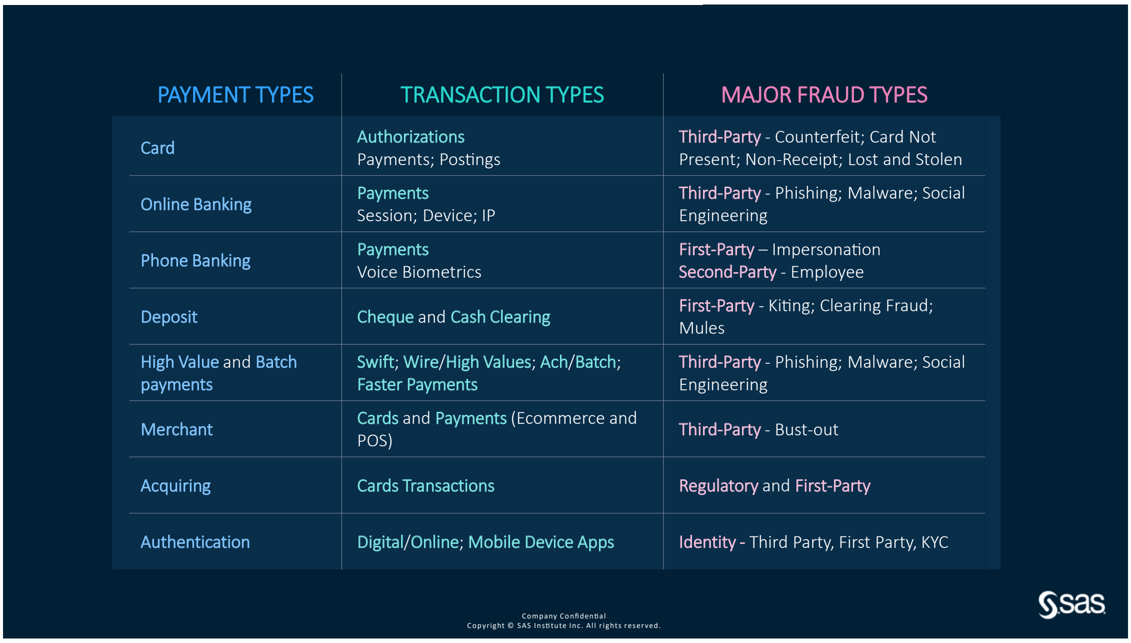
SAS Decisioning Architecture cover risks across fraud, anti-money laundering and credit functions.

Source: SAS

One of SAS' significant differentiators is enterprise decisioning – the ability to make holistic decisions across risk, fraud and marketing on a single architecture that can help to provide a differentiated customer experience (see Figure 2).

SAS' enterprise fraud solution offers end-to-end risk detection built on top of the SAS platform and its analytical capabilities. Proven use cases include financial and non-financial transaction fraud, authentication and validation processes, and identity and verification during customer onboarding (see Figure 3).

Figure 3: SAS' enterprise fraud solution – core typologies

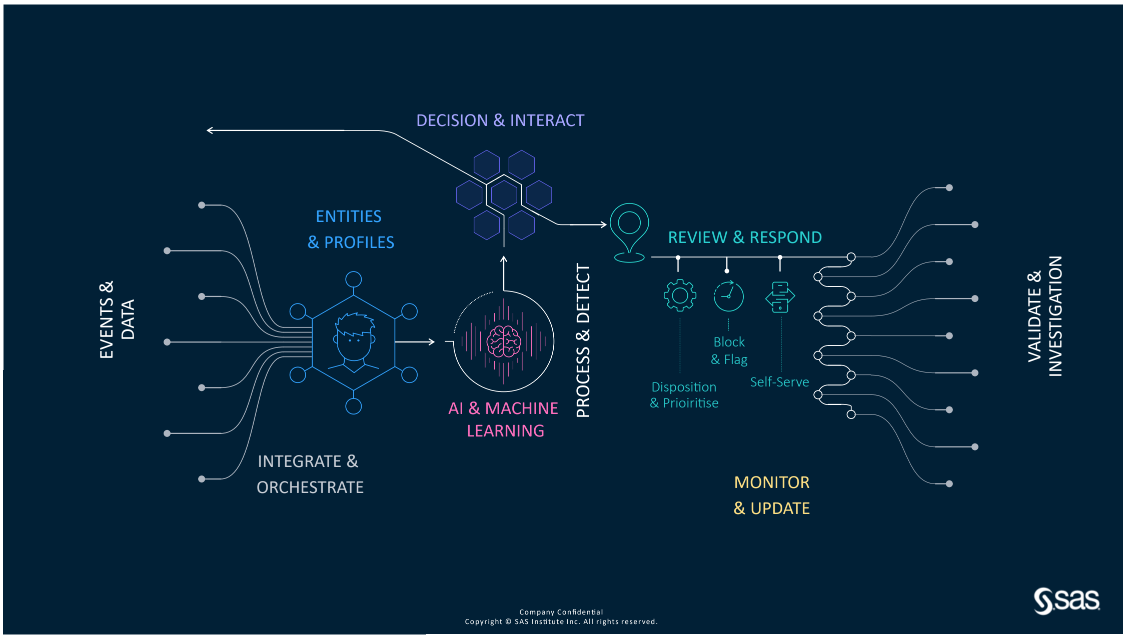


PAYMENT TYPES	TRANSACTION TYPES	MAJOR FRAUD TYPES
Card	Authorizations Payments; Postings	Third-Party - Counterfeit; Card Not Present; Non-Receipt; Lost and Stolen
Online Banking	Payments Session; Device; IP	Third-Party - Phishing; Malware; Social Engineering
Phone Banking	Payments Voice Biometrics	First-Party – Impersonation Second-Party - Employee
Deposit	Cheque and Cash Clearing	First-Party - Kiting; Clearing Fraud; Mules
High Value and Batch payments	Swift; Wire/High Values; Ach/Batch; Faster Payments	Third-Party - Phishing; Malware; Social Engineering
Merchant	Cards and Payments (Ecommerce and POS)	Third-Party - Bust-out
Acquiring	Cards Transactions	Regulatory and First-Party
Authentication	Digital/Online; Mobile Device Apps	Identity - Third Party, First Party, KYC

Company Confidential

Source: SAS

Figure 4: SAS' enterprise fraud solution – workflow elements



Source: SAS

The solution has millisecond processing capabilities that enable risk decisioning in real time, making it ideal for high-speed, high-throughput but low-latency activities that require dynamic profiling and analytics. The solution can also be used for internal F&FC systems. SAS' solution also includes (see Figure 4):

- Profiling Signatures (SAS' patented technology).
- Multiple model processing and rules.
- Support for workflow, work item alerting and risk mitigation in business operations.

SAS' strength lies in its analytics heritage. Designed with analytics at its core, the company's enterprise fraud solution, and also includes the following:

- Development of ML models using a range of supervised and unsupervised techniques that can use SAS or open-source products.
- Deployment and operationalization of models in a real-time (millisecond) processing environment.
- Reporting and dashboard monitoring for key performance indicators (KPIs), both technical/operational and business.
- Deployment of robotic process automation and optimization processes, including prioritization scorecards.

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 Quadrants™ 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.

Briefing process

We conducted face-to-face and/or web-based briefings with each vendor[1] 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 used for the enterprise fraud solutions (2023) report are shown in Table 4.

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,

[1] 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' enterprise fraud solutions (2023) report

Completeness of offering	Market potential
• Advanced/proprietary fraud-detection techniques	• Customer satisfaction
• Behavioral monitoring	• Market penetration
• Libraries of pre-packaged fraud rules	• Growth strategy
• Case management and workflow	• Financials
• Transaction monitoring	
• Identity management capabilities (e.g., device ID, etc.)	

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 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 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.

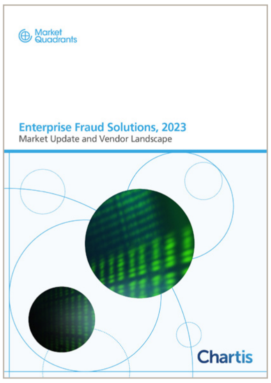
Category leaders

- Category leaders combine depth and breadth of functionality, technology and content with the required organizational characteristics to capture significant share in their market.

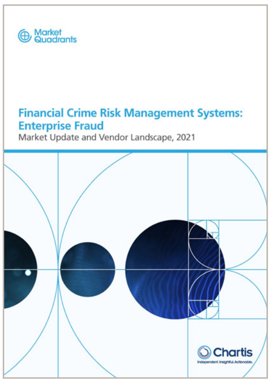
- They demonstrate a clear strategy for sustainable, profitable growth, matched with best-in-class solutions and the range and diversity of offerings, sector coverage and financial strength to absorb demand volatility in specific industry sectors or geographic regions.

- They will typically benefit from strong brand awareness, a global reach, and strong alliance strategies with leading consulting firms and systems integrators.

Further reading


Market Quadrants
Enterprise Fraud Solutions, 2023
Market Update and Vendor Landscape
Chartis

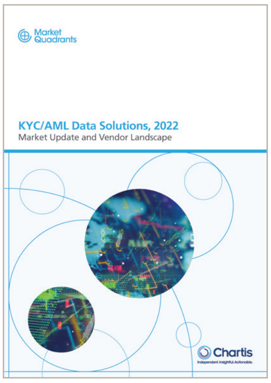
Enterprise Fraud Solutions, 2023: Market Update and Vendor Landscape


Market Quadrants
Financial Crime Risk Management Systems: Enterprise Fraud
Market Update and Vendor Landscape, 2021
Chartis

Financial Crime Risk Management Systems: Enterprise Fraud; Market Update and Vendor Landscape, 2021

Payment Risk Solutions, 2023: Market and Vendor Landscape

KYC Solutions, 2022: Market Update and Vendor Landscape


Market Quadrants
KYC/AML Data Solutions, 2022
Market Update and Vendor Landscape
Chartis

KYC/AML Data Solutions, 2022: Market Update and Vendor Landscape

RiskTech100 2023

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