Chartis

Vendor Analysis: SAS

Enterprise and Payment Fraud Solutions, 2024

Table of contents

List of figures and tables

1. Report context

This Vendor Analysis is based on the Chartis quadrant report **Enterprise and Payment Fraud Solutions, 2024: Market Update and Vendor Landscape** (published in August 2024). This section summarizes the key theses in that report; subsequent sections take a detailed look at SAS's quadrant positioning and scoring, and Chartis' underlying opinion and analysis.

Key thesis

The 2024 Enterprise and Payments Fraud report expands Chartis' previous research to incorporate enterprise and payment fraud as separate market quadrants. The rationale for this arose during the report preparation phase, when interviews with purchasers and users of fraud solutions revealed that the growing complexity of global fraud warranted distinct views of the enterprise fraud and payments fraud market landscapes.

The key distinctions between the two categories are as follows:

- **Enterprise fraud** focuses on a firm's ability to deliver a complete set of anti-fraud functions across the fraud lifecycle, with a specific and designated focus on key fraud typologies.
- **Payment fraud** focuses on vendor specialization in delivering payment rail-specific solutions across the prominent payment channels, with a shift in focus toward real-time fraud detection.

Demand-side takeaways

Context: the evolving fraud landscape

The fraud landscape in 2024 is one of the most challenging the industry has ever faced, and the pace of change is likely to accelerate. Several drivers are shaping the direction of fraud, as well as fraud detection and prevention.

- **Growing, more connected and more globalized fraud activity**. Global fraud activity is growing, not only in volume and velocity but also in complexity and spread, requiring much more sophisticated and flexible countervailing approaches.[1]
- **Regulatory and policy drivers**. Regulators and policymakers are rightly focusing on fraud detection, with several global and regional initiatives (including the liability shift and, more specifically to the UK, new reimbursement policies). In addition to broader fraud regulation, fraud models are coming under growing regulatory scrutiny, so any decisions need to be understood, explainable and free of bias.
- **Customer experience**. Consumer expectations for seamless, fast onboarding, real-time payments and other conveniences are shaping the fraud detection market so that it increasingly aligns with a diverse range of customer journeys. Consumers are also increasingly concerned with understanding the measures that financial institutions are taking to protect them from criminals.

To tackle rising complexity, volume and speed, while also enabling the flexibility to drive good customer experience, financial institutions are increasingly turning to scalable and customizable fraud solutions based on advanced analytics and modeling

With greater complexity, the need to integrate, test and explain increasingly advanced models is critical, and benefits from the power that advanced analytics can bring.

[1] *Global fraud figures are not universally published, but if we take the UK – which does publish figures – as an example, reported fraud losses have dipped somewhat in 2024 (down 4% compared with 2023), offset by stronger growth in prevented fraud (7%). This is without taking into account unreported fraud. There has also been a shift from unauthorized to authorized fraud.*

Vendor Landscape

The global picture

- Global adoption of real-time payments has increased the threat of certain fraud typologies – especially authorized push payment (APP) fraud – with scammers exploiting the ability to defraud their victims and exit the process before any action can be taken. This has heightened the need for real-time payment monitoring and fraud detection. The rise of APP fraud and other 'social engineering' fraud has driven the rise in money mules, through which a significant portion of funds is collected by criminals. This is creating the need for a 'follow the crime' approach, which requires deeper analytics and Big-Data-style approaches, including network analytics.

- As financial institutions recognize the challenges in detecting fraud typologies, this is driving growth in fraud detection at the application and onboarding stages. The key to successfully fighting application fraud lies in firms' ability to integrate a broad set of data and risk signals. We are seeing a strong shift toward platformization, driving strong results in this area.

Europe and the UK

- The situation in Europe and the UK is particularly pressing due to recent regulations regarding liability shifts and reimbursement. Traditionally, victims of fraud bore the brunt of losses in many cases, but this is changing. Banks, payment service providers (PSPs) and others in the financial and commerce ecosystem are attempting to understand not only payee but also receiver accounts – and vendors have responded by building solutions that can be adapted appropriately.

- The UK offers a prime example. Despite **a reported decrease** in APP fraud losses in 2023, the absolute numbers remain high.

- New regulations, such as Payment Services Directive 2 (PSD2) and the upcoming PSD3 in Europe, are placing more responsibility on PSPs for fraudulent APP transactions.

- This shift incentivizes banks and PSPs to invest more heavily in fraud prevention and implement robust fraud detection systems to minimize their losses. But it also creates a potential incentive for victims to report fraud if they believe they will be reimbursed.

- There is nervousness on the part of many institutions that this could also fuel a rise in a new fraud typology – collusion or reimbursement fraud.

Market themes

In our market update, we identified several key themes:

- **The growth in platformization** to empower institutions and provide a better user experience.

- **A focus on modeling** to improve the detection of complex typologies.

- **The transformative influence of low-code/no-code configuration options**, which are enabling custom fraud solutions for the mass market.

- **Growth in application fraud** as an early-warning signal.

- **Generative artificial intelligence (GenAI)** – powering automation and co-piloting tasks.

Supply-side takeaways

Anti-fraud solutions are evolving to the point where they now balance customization and scalability. While regional tailoring remains crucial, leading vendors offer focused solution capabilities across multiple fraud typologies, industries and geographies. This shift has made a strong global presence, robust support services and a replicable, profitable business model essential for success. Indeed, these qualities are now considered 'table stakes' – the minimum requirement to compete in the market. Industry-leading vendors increasingly face competition from nimble startups offering innovative solutions. They are responding by maintaining a continuous focus and investing significant resources into critical areas to strengthen their offerings and maintain market share.

Anomaly detection and rules around monitoring financial and non-financial transactions remain the foundation of anti-fraud solutions. But leading vendors go beyond this, prioritizing low latency for real-time monitoring and analysis.

In addition, category-leading solutions typically offer comprehensive monitoring across multiple channels, including mobile, alternative, peer-to-peer and check payments. This holistic view of customer behavior enables financial institutions and vendors to detect fraudulent activity that might be missed by focusing on a single channel.

2. Quadrant context

Introducing the Chartis RiskTech Quadrant®

This section of the report contains:

- The Chartis RiskTech Quadrants® for enterprise and payment fraud solutions, 2024.
- An examination of SAS's positioning and its scores as part of Chartis' analysis.
- A consideration of how the quadrant reflects the broader vendor landscape.

Summary information

What does the Chartis quadrant show?

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 enterprise and payment 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 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 described 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 Quadrants® for enterprise and payment fraud solutions, 2024

Figures 1 and 2 illustrate Chartis' view of the vendor landscapes for enterprise and payment fraud solutions, highlighting SAS's position.

Figure 1: RiskTech Quadrant® for enterprise fraud solutions, 2024

Source: Chartis Research

Quadrant dynamics

General quadrant takeaways

Leading vendors are focusing on improving the agility of their solutions via deep layers of configurability. They are also putting customization in the hands of clients – whether via no-code interfaces or other approaches, to enable fast and easy modifications and updates in response to evolving fraud threats and patterns.

Figure 2: RiskTech Quadrant® for payment fraud solutions, 2024

Source: Chartis Research

More self-service analytics can help financial institutions take control of their fraud defenses by tailoring detection and prevention strategies to their unique regulatory and geographical needs and requirements, and moving beyond the limitations of pre-packaged solutions. Moreover, by leveraging their in-house expertise and resources, institutions can achieve greater cost-efficiency and streamline their fraud prevention efforts.

Our research also highlights growth in platformization and connectivity with third parties via application programming interface (API) integrations, giving financial institutions a centralized way to access data and functionality from all anti-fraud measures. This approach also lends itself to scalability and flexibility, allowing institutions to scale up or down as needed.

Vendor positioning in context – completeness of offering

SAS's category leader status in enterprise and payment fraud reflects its deep expertise and focus across the fraud lifecycle.

SAS's ability to scale and customize across the full fraud cycle stems first and foremost from the power of its end-to-end enterprise platform. This enables the use of advanced fraud detection and analytical techniques that operate across enterprise and payment fraud. A deep analytics tech stack enables

multi-layered detection that can be a hugely effective way to detect genuine fraudulent activity and reduce noise (including false positives). The platform provides a fully configurable business orchestration layer, enabling integrations with a large pool of data (via analytics or third-party data providers), enriching this with device data and biometrics to create a real-time detection engine.

SAS has developed extremely strong modeling capabilities in its deep libraries of pre-packaged fraud models and typologies, and in developing and managing models via its advanced modeling studio. Indeed, SAS received a high rating for its libraries of pre-packaged fraud rules and typologies, which can enable firms to tune their approach not only to their risk appetite but also to the very specific requirements of individual typologies (and sub-typologies), payment channels and vertical and horizontal focuses. With wide coverage across the spectrum of fraud typologies, these libraries begin with 'starter rules' based on industry trends that firms can use on implementation. Firms can then customize and adjust fraud rules to meet a company's compliance requirements via SAS's fraud rules 'authoring' and 'testing' interface. The enterprise fraud solution is designed as an end-to-end risk detection and analytics platform that provides capabilities across all the components required for the end-to-end prevention, detection and investigation of fraud.

SAS's solution provides strong packaging, again focused around rules, models and analytics, with a flexible set of deployment options. This reflects the high rating it received in this area, which is particularly compelling when the breadth of SAS's client base and its relative customer needs are considered. SAS's solution simplifies data integration, enabling firms to combine all internal, external and third-party data to create better predictive models for their particular fraud detection and prevention needs. By combining this data onto a single technology platform, firms have the flexibility to scale as they change and respond to new fraud trends. Moreover, as workflows improve and the technology generates fewer false positives, firms can provide a better customer experience while detecting more instances of fraud. The solution's embedded machine learning (ML) capabilities are programmed to detect and adapt to changing behavioral patterns, resulting in more effective, versatile models.

Leading vendors in this space are increasingly deploying GenAI across different use cases (such as creating synthetic data, interpreting large, unstructured data, or automating workflow with co-pilots). SAS has advanced capabilities across all these domains and provides a range of out-of-the box options. It also enables firms to build and customize GenAI capabilities in scenarios where an added layer of customization is required.

When it comes to fraud typologies, SAS has a highly advanced approach and solution to two of the fastest-growing yet hardest to detect typologies: APP fraud and money muling. For these typologies, SAS combines a number of behavioral, geographic, transactional and account signals and layers on link analysis and other deep analytical and ML/AI techniques. This is done across the lifecycle, enabling a holistic and interconnected view that is increasingly required for APP and mule detection. The ability to do this in real time means that SAS can adapt well to very complex and high-scale use cases.

In payment fraud, Chartis' high rating for SAS's solutions was based on several factors, notably their ability to deliver scalable fraud detection across a myriad of payment rails, and their ability to hit extremely high detection speeds and volumes. Both factors are considerable strengths when responding to the modern payments ecosystem, in which consumers are relying more on real-time payments.

Chartis believes that certain elements enable SAS to meet demand. The solutions' 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 and make decisions about every transaction in real time.

As in enterprise fraud, SAS's platform, together with the strength of its modeling and analytics, enable scalability and flexibility. SAS provides a deep set of features in its enterprise fraud solution offering, allowing it to offer strong capabilities in almost every area of enterprise and payment fraud. This contributed significantly to the company's position as a category leader.

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

Table 1: Completeness of offering – SAS (enterprise and payment fraud solutions, 2024)

Completeness of offering criteria – enterprise fraud solutions	Coverage
Core technology	
Advanced/proprietary fraud-detection techniques	High
Behavioral monitoring	High
Libraries of pre-packaged fraud rules	High
Modeling and testing	High
Solution packaging and deployment	High
Platform, workflow and analytics	High
Fraud typologies	
Application fraud and identity risk	High
APP and social engineering	High
Mule detection	High
Cyber and others	High
Completeness of offering criterion – payment fraud solutions	**Coverage**
Core technology	
Fraud typologies	High
Speed, volume and performance	High
Fraud and analytical models	High
Solution packaging and deployment	High
Payment rails	
Card payments	High
Real-time payments	High
Other A2A/Wire payments	High
ACH fraud	High
Check fraud	High
Alternative payments	High

Source: Chartis Research

Vendor positioning in context – market potential

SAS's enterprise and payment fraud solutions have become established as leaders in fraud detection and prevention services, and this success contributed significantly to the vendor's position as a category leader in both RiskTech Quadrants®.

In particular, the strong ratings for customer success and market penetration reflect the company's large, global and diversified client base, which comprises a variety of firms, including but not limited to, banks, PSPs and FinTechs.

SAS's high ratings for growth strategy and financials are evidence of the increasing demand for its services and solutions across North America, Europe, the Middle East and Africa (EMEA) and Asia-Pacific – and have helped to boost client acquisitions. To keep up with expanding demand, SAS has widened its client base across all tiers and areas of focus, and increased its already extensive workforce.

Chartis also found SAS's product and strategic roadmap to be highly compelling and in tune with the direction of the markets it serves.

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

Table 2: Market potential – SAS (enterprise and payment fraud solutions, 2024)

Market potential criteria – enterprise fraud solutions	Coverage
Customer satisfaction	High
Market penetration	High
Growth strategy	High
Financials	High
Market potential criterion – payment fraud solutions	**Coverage**
Customer satisfaction	High
Market penetration	High
Growth strategy	High
Financials	High

Source: Chartis Research

3. Vendor context

Overview of relevant solutions/capabilities

SAS is a leader in business analytics software and services, and the largest independent vendor in the business intelligence market. Since 1976, SAS has helped customers at more than 80,000 sites around the world improve their performance and deliver value by making better decisions faster.

SAS's Risk, Fraud and Compliance Solutions (RFCS) take a unified approach, delivering an essential layer of protection backed by domain expertise and advanced analytics.

Table 3 gives an overview of SAS and its enterprise and payment fraud solutions.

Table 3: SAS – company information

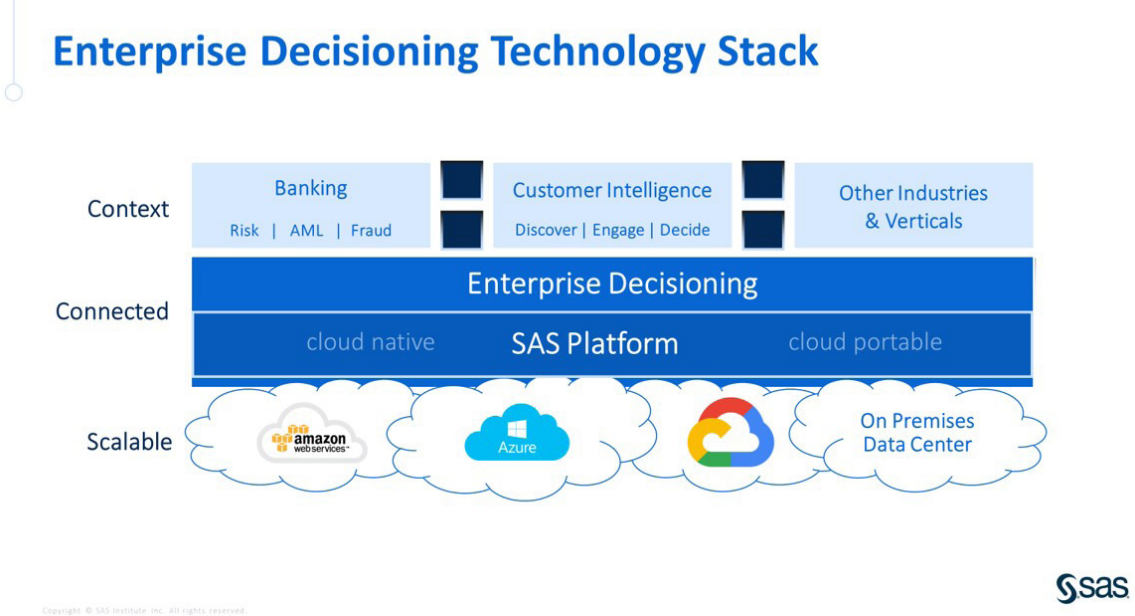
Company	SAS
Headquarters	Cary, NC, US
Other offices	SAS has offices in 56 countries worldwide.
Description	SAS is a leading data and AI provider and one of the largest privately held software companies in the world. Used by 91 of the top 100 companies in the global Fortune 500, SAS aspires to be the most trusted provider of AI solutions in the market. SAS's enterprise fraud solution capitalizes on decisioning capabilities that span all areas of fraud, compliance and credit risk, as well as marketing intelligence. These are designed and built by dedicated SAS R&D teams, with embedded AI capabilities at the forefront to facilitate the effective mitigation of identified risks. Across the RFCS portfolio, the solutions optimize common capabilities, beginning with intelligent data orchestration and enrichment, 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 performed via flexible alert triage and a case management interface.
Solution	Although modular, SAS's enterprise fraud solution offers tightly integrated components with an end-to-end risk capability. SAS ensures that a financial institution can detect, identify, prevent and validate threats from external and internal sources. The holistic advanced analytics that SAS applies via its AI and ML capabilities, within a strong development, governance and deployment mechanism, continue to be core to the solution. This enables clients to deal with attacks while meeting model risk governance expectations. Underpinned by a cloud-native platform, the solutions are designed to satisfy demand for the increasing volumes of data that firms need to consume remote channel information at high throughput and low latency.

Source: SAS

SAS was founded in 1976 and continues to be led by co-founder and CEO Jim Goodnight. The company focuses on analytics, data science and ML; over the decades, this has grown to touch on specializations across multiple industries. SAS's fraud and financial crimes (F&FC) solutions are used by 300 financial institutions globally, many of them using SAS for both fraud and compliance. In addition, two-thirds of global systemically important banks (GSIBs) use SAS for F&FC solutions. Total revenue growth in the fraud operations unit was in double digits in 2023.

One of SAS's major differentiators is enterprise decisioning – the ability to make holistic decisions across risk, fraud and marketing on a single architecture (see Figure 3). This capability can provide a differentiated customer experience that can set an organization apart.

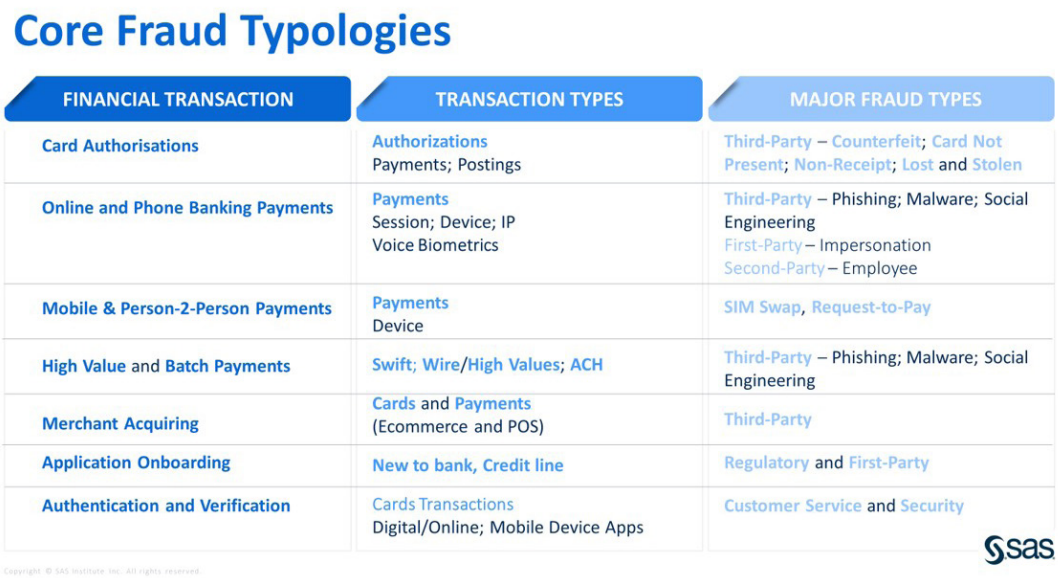
Figure 3: SAS RFCS decisioning architecture



Source: SAS

SAS's enterprise fraud solution offers end-to-end risk detection built on top of the SAS platform and its analytical capabilities (see Figure 4 on page 14). Proven use cases include financial and non-financial transaction fraud, authentication and validation processes, and identity and verification during customer onboarding.

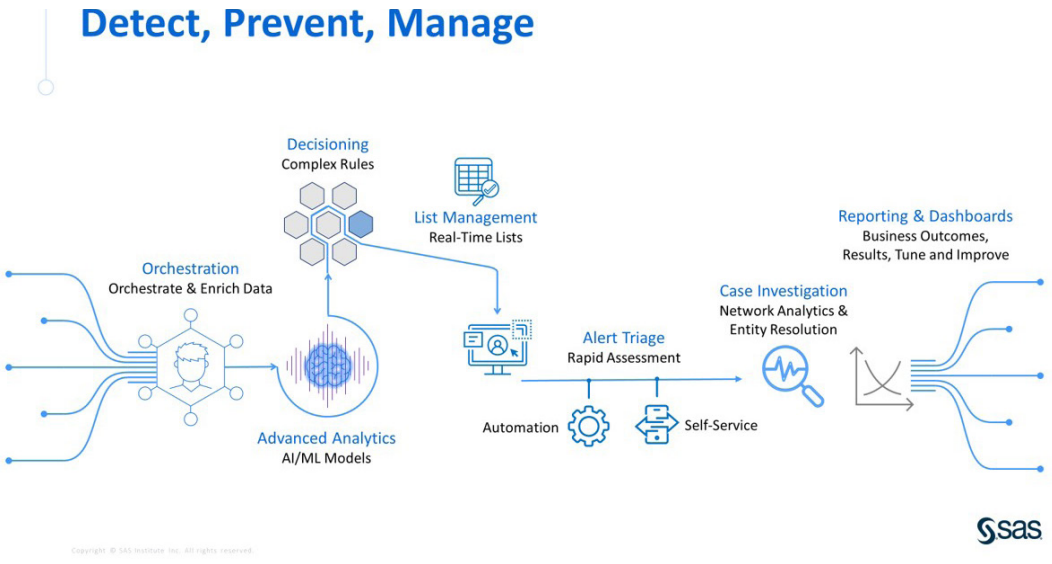
Figure 4: Core typologies



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. SAS's enterprise fraud solution includes profiling signatures (SAS's patented technology) and multiple model processing and rules, and covers business operations for which it supports workflow, work item alerting and risk mitigation (see Figure 5).

Figure 5: SAS's enterprise fraud solution



Source: SAS

Vendor Landscape

SAS's strength is in its analytics heritage. Its enterprise fraud solution is designed with analytics at the core and includes:

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

Vendor leading practices

- End-to-end solutions across the financial crimes spectrum. SAS has reinvested more than a billion dollars in R&D to rearchitect its fraud and financial crimes solutions on a common cloud-native decisioning platform. The system supports anti-money laundering (AML) transaction monitoring, customer due diligence, sanctions, identity and verification, payment fraud monitoring and non-transactional fraud detection, supported by a unified case management capability.
- Data orchestration of digital signals for inclusion in SAS's patented signatures. This allows firms to integrate geolocation, device intelligence and biometric data to monitor digital payments, uncover synthetic identities and improve value detection rates more accurately.
- Design-time analytic user interfaces support the deployment of SAS and open-source (Python, R, etc.) models through a model pipeline user interface. The low-code/no-code interface empowers data scientists to challenge multiple modeling techniques supported by AI-generated documentation and model scorecards that help to explain strategies.
- A guided rules analysis interface enables fraud strategists to make intraday adjustments to alert handling, routing and queueing processes. The system also supports estimation or impact analysis to predict the operational impact of changes in strategies.
- The domain expertise of industry practitioners differentiates the customer experience. SAS routinely conducts periodic 'health checks' with customers to share trends and best practices, as well as knowledge transfer to ensure that clients can sustain their fraud strategies.

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 industries, including banking, insurance and capital markets. The findings and analyses in its quadrant reports reflect its 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 its 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

Chartis conducts face-to-face and/or web-based briefings with each vendor.[2] 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

Chartis develops 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, Chartis can ensure transparency in its methodology and allow readers to fully appreciate the rationale for its analysis. The specific criteria used for the Enterprise and Payment Fraud Solutions, 2024 report are shown in Table 4 on page 17.

[2] *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 and payment fraud solutions, 2024 report

Completeness of offering	Market potential
Enterprise fraud solutions:	Customer satisfaction
Core technology	Market penetration
Advanced/proprietary fraud-detection techniques	Growth strategy
Behavioral monitoring	Financials
Libraries of pre-packaged fraud rules	
Modeling and testing	
Solution packaging and deployment	
Platform, workflow and analytics	
Fraud typologies	
Application fraud and identity risk	
APP and social engineering	
Mule detection	
Cyber and others	
Payment fraud solutions:	
Core technology	
Fraud typologies	
Speed, volume and performance	
Fraud and analytical models	
Solution packaging and deployment	
Payment rails	
Card payments	
Real-time payments	
Other A2A/Wire payments	
ACH fraud	
Check fraud	
Alternative payments	

Source: Chartis Research

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, 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 the 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 particular users' needs.

Point solutions

- Point solution 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.

Vendor Landscape

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 a 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.