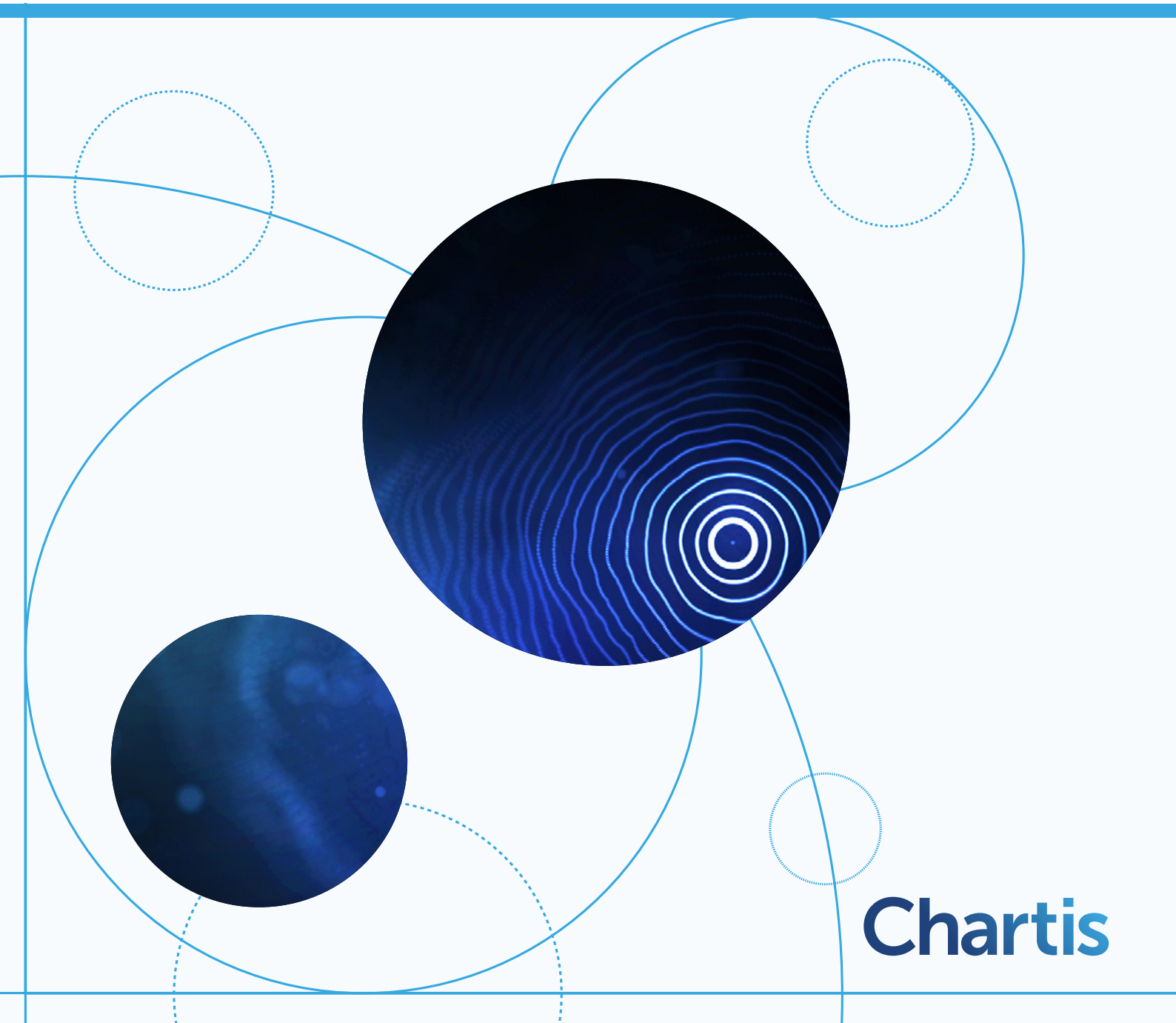
Market Quadrants

Enterprise and Payment Fraud Solutions, 2024

Market Update and Vendor Landscape



Chartis

About Chartis

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

- Credit risk.
- Operational risk and governance, risk management and compliance (GRC).
- Market risk.
- Asset and liability management (ALM) and liquidity risk.
- Energy and commodity trading risk.
- Financial crime, including trader surveillance, anti-fraud and anti-money laundering.
- Cyber risk management.
- Insurance risk.
- Regulatory requirements.
- Wealth advisory.
- Asset management.

Chartis focuses on risk and compliance technology, giving it a significant advantage over generic market analysts.

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

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

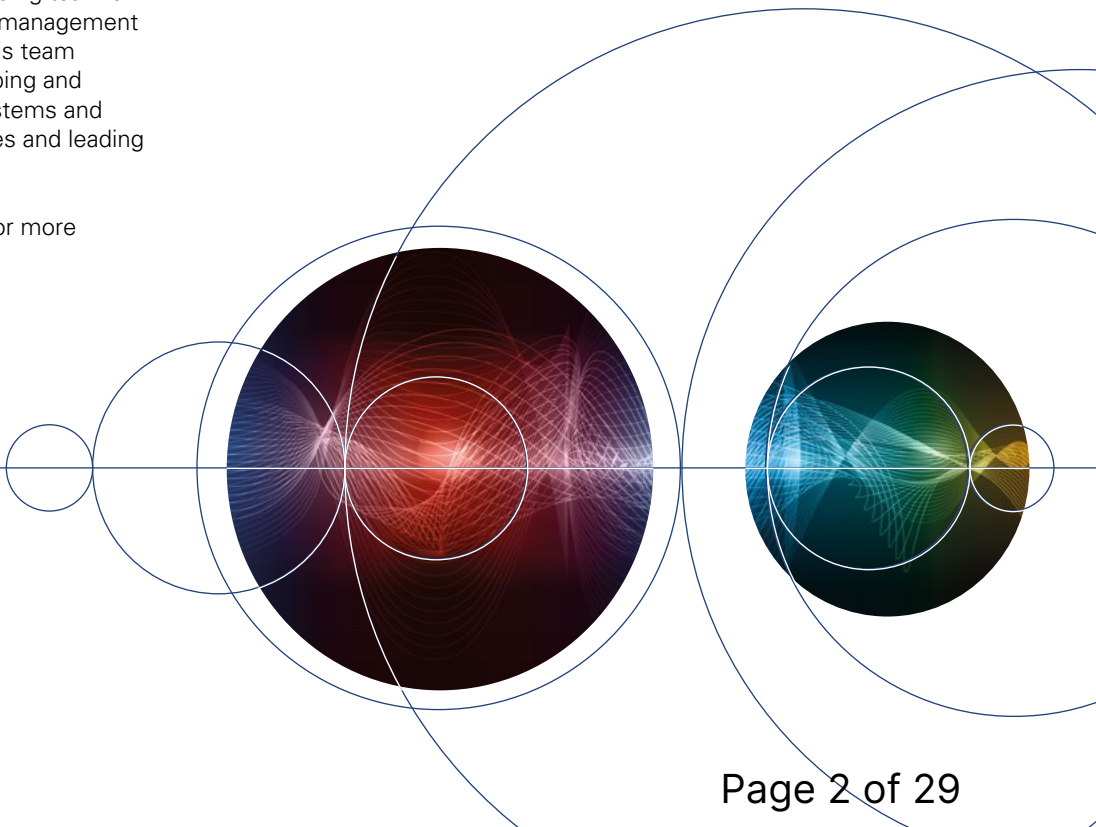
© Copyright Infopro Digital Services Limited 2024. All Rights Reserved.

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

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

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

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



09 AUG 2024

Market Quadrants Report

Author
Nick Vitchev, Phil Mackenzie, Jason Wright and Ahmad Kataf

Jump to: Market update | Vendor landscape | Chartis RiskTech Quadrants® and tables | Methodology

Executive summary

This report updates *Enterprise Fraud Solutions, 2023: Market Update and Vendor Landscape* and *Payment Risk Solutions, 2023: Market and Vendor Landscape*, taking key themes from both reports. We have examined the fraud landscape through both lenses following feedback from end users, including banks, payment service providers (PSPs), FinTechs and others outside the financial ecosystem. It became clear that these distinct areas should be viewed together, along with the more granular breakdown of offerings within them.

In our view, the main distinction between enterprise and payment fraud is that enterprise fraud focuses on a firm's ability to deliver a complete set of anti-fraud functionalities, with a focus on fraud typologies (whether origination, authorized push payment [APP] or cyber fraud), as well as the stages in the customer lifecycle that each vendor touches. The payment fraud quadrant in this report, meanwhile, focuses on the specialization of vendors across different payment channels.

This update covers several key themes in the market for anti-fraud solutions, notably around 'platformization', low-code/no-code configuration, the embedding of such typically siloed solutions as identity verification (IDV) into an interconnected workflow, and generative artificial intelligence's (GenAI) growing role in automation and the co-piloting of fraud solutions.

The fraud landscape is constantly changing, and financial institutions, along with technology providers, are racing to develop better and more flexible tools to keep up. In addition, regulators are now emphasizing the importance of managing the risk associated with these models. This means that

financial institutions and vendors need to integrate, test and explain increasingly complex models, while also tackling the challenge of analyzing and interpreting massive amounts of data.

Institutions are increasingly turning to fraud tools and solutions to reduce risk, ensure compliance and protect their reputations. By leveraging cutting-edge technology and working strategically, vendors can create solutions that address their clients' ever-changing needs and even give them a competitive edge.

This report uses Chartis' RiskTech Quadrant® to explain the structure of the market. The RiskTech Quadrant® employs a comprehensive methodology of in-depth independent research and a clear scoring system to explain which technology solutions meet an institution's needs. The RiskTech Quadrant® does not simply describe one technology solution as the best; rather, it has a sophisticated ranking methodology to explain which solutions would be most suitable for buyers, depending on their implementation strategies.

This report covers the following providers of enterprise and payment fraud solutions:[1] Abrigo, BPC, Clari5, DataVisor, Effectiv, Feedzai, FICO, FIS, Focal, IDVerse, INFORM, LexisNexis Risk Solutions, Lynx, Manipal Group, Minerva, Nasdaq Verafin, NetGuardians, NICE Actimize, Quantexa, Refine Intelligence, Rozes, SAS, Sumsub, SymphonyAI, Tookitaki and Veriff.

We aim to provide as comprehensive a view of the vendor landscape as possible within the context of our research. Note, however, that not all vendors we approached provided adequate information for our analysis, and some declined to participate in this research.

Jump to top

Market update

Context: the evolving fraud landscape

Fraud continues to evolve. In recent years, APP fraud has become a growing concern globally, particularly in Europe and the UK, where incidents have spiked. This surge can be attributed in part to a recent shift in liability and reimbursement policies:

The global picture

- Faster payment adoption worldwide has created fertile ground for APP fraud schemes. Scammers exploit faster payment systems to trick victims into authorizing fraudulent transactions.
- Reports indicate significant losses due to APP scams.

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 that is changing. Banks, 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.
- While this shift incentivizes banks and PSPs to invest more heavily in fraud prevention and implement robust fraud detection systems to minimize their losses, 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 the rise of a new fraud typology – collusion or reimbursement fraud.

> #### Reimbursement/collusion fraud: the unintended consequence of shifted liability
>
> The rise of APP fraud and the subsequent shift in liability toward PSPs have led to an unintended consequence: the emergence of a new fraud typology, reimbursement/collusion fraud. This exploits the potential laxity in reporting due to reimbursement policies, and can induce the following actions and events:
>
> - Collusion between a victim (knowingly or unknowingly) and a fraudster.

- The fraudster initiates a fraudulent APP transaction from the victim's account.
- The victim, aware of the reimbursement policy, reports the fraud. However, they may delay doing this, to allow the fraudster to benefit from the funds before the transaction is flagged.

If victims are slow to report fraudulent activity, reimbursement/collusion fraud can undermine efforts to track and prosecute actual fraudsters. This type of fraud also increases the costs for PSPs that reimburse fraudulent claims.

Mitigating reimbursement/collusion fraud: a multi-faceted approach

- **Consumer education**. Financial institutions and regulators need to educate consumers about the dangers of colluding with criminals and the impact this could have on their financial and physical wellbeing going forward. Similar efforts are being made to educate those most at risk about the dangers of becoming a money mule.
- **Refined reimbursement policies**. PSPs should explore ways to incentivize prompt reporting, perhaps through faster reimbursements or tiered systems based on reporting speed.
- **New rules and techniques** tailored to reimbursement or collusion fraud detection are needed. Greater scrutiny of victims' activity will likely be required, as well as the exposure of known reimbursement fraud networks.
- **Advanced fraud detection**. Continued development of robust fraud detection systems by PSPs is crucial to identify and prevent fraudulent APP transactions before they occur.

Market themes

In this update, we have identified several key themes, explored in more detail below:

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

- **The transformative influence of low-code/no-code configuration options**, which are enabling custom fraud solutions for the mass market.
- **ID risk detection** as an early warning signal.
- **GenAI** – powering automation and co-piloting tasks.

The growth in platformization

As fraud detection and prevention become more complex, firms are moving away from tightly defined fraud and compliance silos toward a deeper and broader understanding and mitigation of financial crime risk. In this context, Chartis is seeing the growing availability – and popularity – of platforms, and an increase in platformization across the fraud market. Platformization in enterprise and payment fraud prevention is essentially the shift from siloed tools and point solutions to a unified environment for managing all anti-fraud activities. This is especially noticeable in the convergence of fraud and credit within retail finance, for example, or the integration of Know Your Customer (KYC) and anti-money laundering (AML) systems.

This approach is gaining significant traction, notably among mid-tier banks and FinTechs in Europe, the Middle East and Africa (EMEA), due to its ability to scale and adapt to rapidly changing requirements. As organizations look to add risk typologies, whether to account for geographic or line-of-business expansion, platforms can support this while still managing to connect to a workflow or ecosystem.

The key benefits of platformization include:

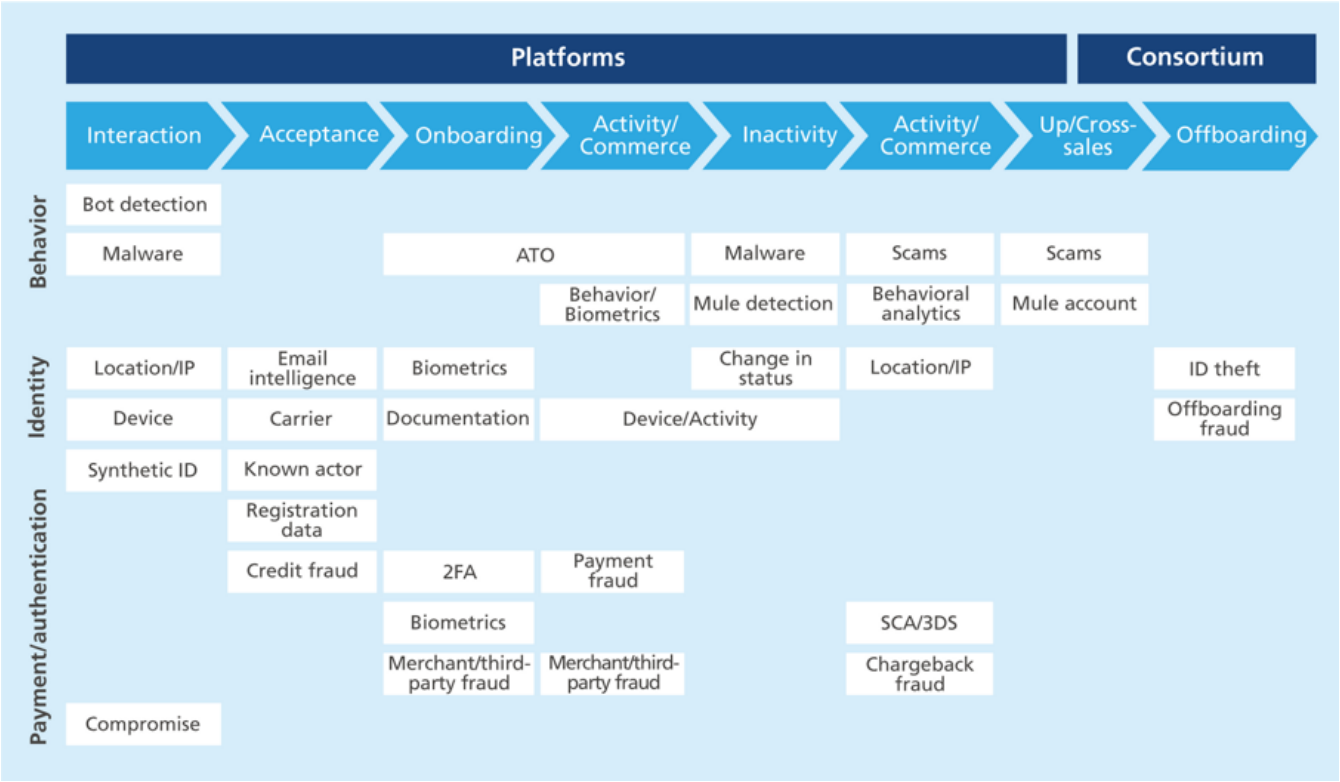
- **A centralized approach**, with all fraud detection and prevention tools in one place. A platform eliminates the need to juggle multiple point solutions and brings together data, tools and functionalities into a single system. This simplifies operations for fraud analysts, improves efficiency and enables a more holistic view of potential threats.
- **A scalable and flexible solution** that allows financial institutions to remain agile when dealing with constantly evolving and innovative fraud techniques. Platforms are designed to be scalable (up or down), so institutions can easily add or remove features and functions as the business grows, the threat landscape changes or the regulatory landscape evolves.
- **Improved collaboration and enhanced data sharing and analytics**,

because a platform provides a central location for information sharing across the institution. Traditionally, data from different departments within an enterprise has been kept separate within different point solutions. Platformization offers a comprehensive view of customer behavior and transactions, enabling more effective fraud detection through advanced analytics and machine learning (ML). This approach also streamlines investigations, enabling firms to resolve fraudulent activities faster.

- **Openness to application programming interface (API) integrations** with external third-party data sources, such as fraud databases and industry threat intelligence feeds. This enriches the platform's capabilities and provides a more comprehensive picture of potential threats. For instance, by integrating systems with a credit bureau database, firms can gain valuable insights into customers' credit history and potential risks.

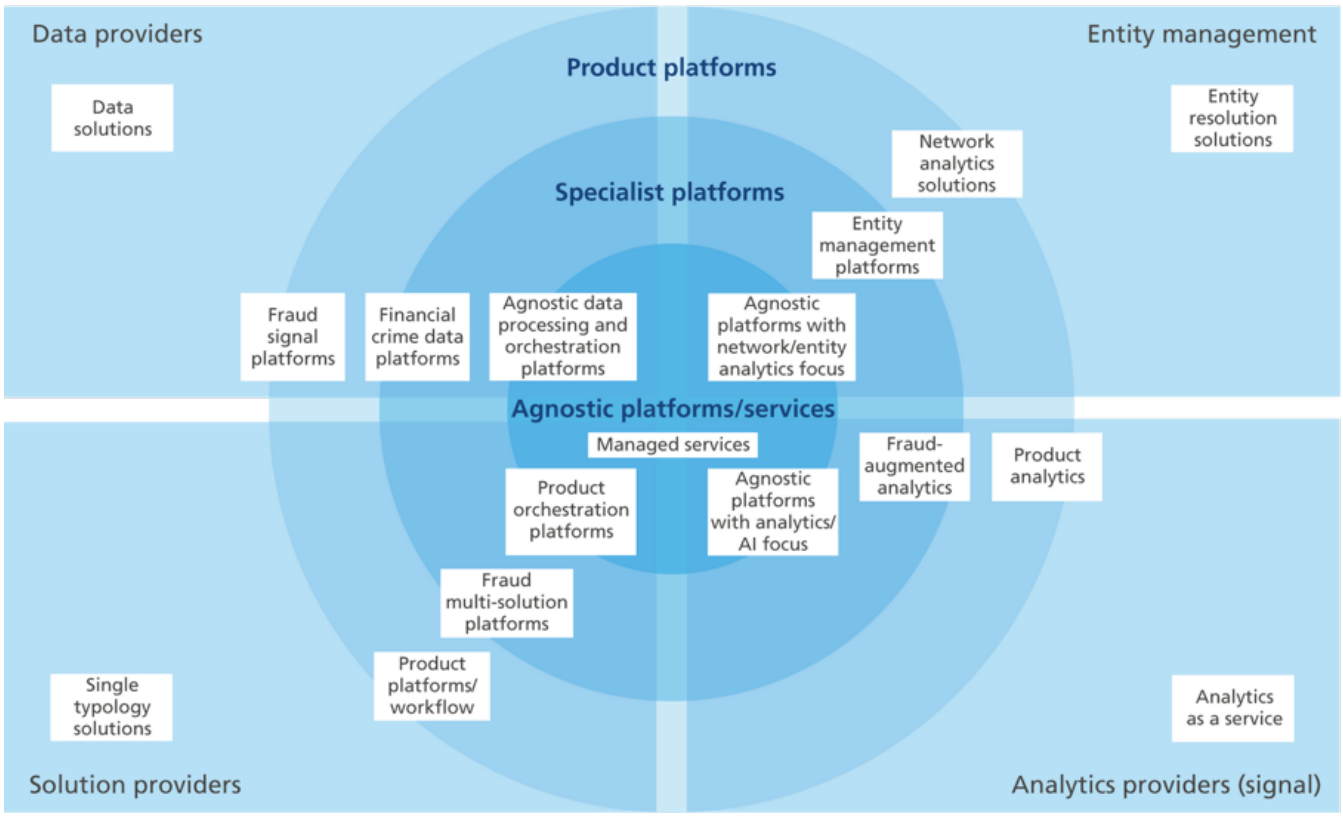
Figure 1 shows how a fragmented fraud tech stack can be combined and integrated across the customer lifecycle via platformization. And because there are many different interpretations of the term 'platform', we are seeing a broad range emerge, from 'agnostic' platforms to highly specific product platforms (see Figure 2).

Figure 1: Platforming anti-fraud capabilities – multiple touchpoints throughout the customer lifecycle



Source: Chartis Research

Figure 2: Fraud platforms – a broad range



Source: Chartis Research

The transformative influence of low-code/no-code configuration options

Low-code/no-code solution configurations are transforming the way that firms approach enterprise and payment fraud solutions. These platforms and solutions allow institutions to build and customize fraud detection and prevention tools without the need for extensive coding expertise, or a long wait to have a solution customized. As low-code/no-code technology matures, we expect to see even greater customization and transparency. Low-code/no-code solutions offer several benefits, including:

- **The democratization of fraud detection and prevention**. Traditionally, building and maintaining a fraud solution required a team of skilled developers and a large IT infrastructure. Low-code/no-code solutions remove this barrier by providing user-friendly interfaces with drag-and-drop functions and pre-built components. Industry-leading vendors provide their customers with a sandbox environment to test any new changes before they go live into production, to ensure their solution matches the institution's risk appetite.

- **Cost-effectiveness**, making platforms accessible to the mass market. Developing custom-built fraud solutions from scratch can be expensive and time-consuming. By reducing reliance on professional developers and streamlining the process, institutions can save on development costs and deploy their fraud solutions faster.
- **Rapid response to evolving fraud**. As fraud schemes are constantly evolving and becoming ever more elaborate, a low-code/no-code platform enables institutions to adapt quickly. With minimal coding, fraud teams can modify existing workflows or build new ones to address emerging fraud schemes.

However, it is important to remember that low-code/no-code solutions have their limitations. Complex fraud scenarios or highly customized integrations may still require vendor or developer involvement, while ensuring robust security measures within low-code-/no-code applications is vital.

ID risk detection as an early warning signal

IDV and other identity-related risk management tools can and should be used throughout the customer lifecycle. However, they can be very useful in delivering fraud signals early in an interaction. IDV can play a vital role within enterprise and payment fraud solutions by acting as the first line of defense against unauthorized access and fraudulent transactions, verifying user identities, combating synthetic ID fraud and ensuring regulatory compliance.

At their core, IDV solutions ensure that a person attempting a transaction is who they claim to be. This involves verifying government-issued IDs, passports or drivers' licenses against official databases and checking for inconsistencies or signs of manipulation. By confirming a user's legitimate identity, IDV helps prevent account takeover attempts and impersonation fraud. Firms in many industries, and especially financial and banking institutions, are subject to strict KYC regulations. IDV solutions can help institutions comply with these by ensuring they have a clear picture of who their customers are.

Many IDV providers offer flexible and scalable solutions, often integrating a risk-based approach, and for low-risk transactions, a simple ID check might suffice. For high-value transactions or users with suspicious activity, however, additional verification steps (such as 'liveness' checks or document cross-referencing) can be triggered.

Synthetic identity fraud in Europe: a growing threat

Synthetic identity fraud is a form of application fraud whereby fraudsters create fake identities by combining real and fabricated information. While this has long been a significant fraud threat in North America, primarily the US, we are seeing evidence that it is growing in Europe and beyond. Europe in particular offers fertile ground for this type of fraud, for several reasons:

- European data privacy regulations (such as the General Data Protection Regulation [GDPR]) restrict data sharing between entities. This data fragmentation can make it more difficult for institutions and IDV providers to verify the authenticity of information provided by applicants.
- European countries often have multiple ID formats and a variety of verification processes. This complexity can create challenges for institutions in implementing robust IDV procedures consistently.
- Europe's rapid shift toward online services makes it easier for fraudsters to exploit weaknesses in digital application processes.
- Automation and the use of technology such as GenAI are causing the market to be flooded with low-cost synthetic IDs.
- Trading places on the dark web are now so effective that the mass production of synthetic IDs can be highly lucrative.

Fraudsters use synthetic IDs in various application fraud schemes, including account takeover, new account fraud (loans, credit cards), mobile phone contract fraud and synthetic mule fraud, whereby criminals use synthetic identities to receive and launder stolen funds. Fraudsters can also exploit KYC procedures to open bank accounts.

Combating synthetic ID fraud in Europe

- Stricter IDV procedures are being implemented, including document verification, facial recognition, liveness verification and address confirmation.

- Specialist solutions are emerging. These aim to identify and block the use of synthetic IDs tailored to the European market, and often use historical data and analytical tools.
- Banks are reviewing historical account data in an effort to identify synthetic IDs and understand constructs and patterns to help with identification and prevention.
- Institutions are exploring ways to share relevant data securely to improve their IDV capabilities, while complying with European data privacy regulations.
- More collaboration between financial institutions and law enforcement agencies is needed to share information and develop joint strategies.
- Firms are using advanced analytics and ML to identify suspicious application patterns that might indicate fraudulent activity.

Ultimately, by understanding the unique European landscape and the methods used by fraudsters, and by implementing robust countermeasures, financial institutions can protect themselves (and their customers) from financial loss, reputational damage and regulatory scrutiny.

GenAI: powering automation and co-piloting tasks

We are seeing some innovative use of GenAI in combating enterprise and payment fraud, mainly via automation and co-piloting. GenAI is not designed to replace human analysts, but rather to work alongside them, providing real-time insights, suggesting potential leads and helping analysts make more informed decisions. Applications for GenAI can include highlighting suspicious transactions or automatically generating a risk profile for a particular customer.

Nevertheless, GenAI is a relatively new and developing technology, and its use in enterprises is evolving. But given its significant potential benefits, we can expect to see more widespread adoption of this technology in the coming years.

Jump to top

Vendor landscape

Overview and key dynamics

Anti-fraud solutions are evolving to the point where they balance customization and scalability. While regional tailoring remains crucial, leading vendors are those that can 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 start-ups offering innovative solutions, and all vendors are now investing significant resources into critical areas to strengthen their offerings and maintain market share.

Leading vendors are also focusing on improving the agility of their solutions through low-code/no-code configurability, to enable fast and easy modifications and updates in response to evolving fraud threats and patterns. And growth in 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 the growth of platformization and connectivity with third parties via 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.

While transactions, payments and data monitoring remain the foundation of anti-fraud solutions, leading vendors go beyond this by 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.

Jump to top

Chartis RiskTech Quadrants® and vendor capabilities for enterprise and payment fraud solutions, 2024

Figures 3 and 4 illustrate Chartis' view of the vendor landscapes for enterprise and payment fraud solutions. Tables 1 and 2 list the completeness of offering and market potential criteria we used to assess the vendors in each category. Tables 3 to 6 list the respective vendor capabilities in the areas we analyzed. In each category, we separated core capabilities from specific capabilities: fraud typologies (for enterprise fraud) and payment rails (for payment fraud).

Figure 3: RiskTech Quadrant® for enterprise fraud solutions, 2024



Source: Chartis Research

Figure 4: RiskTech Quadrant® for payment fraud solutions, 2024



Source: Chartis Research

Table 1: Assessment criteria for vendors of enterprise fraud solutions, 2024

Completeness of offering	Market potential
Core technology	Customer satisfaction
Advanced/proprietary fraud-detection techniques	Market penetration
Behavioral monitoring	Growth strategy
Libraries of pre-packaged fraud rules	Business model
Modeling and testing	Financials
Solution packaging and deployment	
Platform, workflow and analytics	
Fraud typologies	
Application fraud and identity risk	
APP and social engineering	
Mule detection	
Cyber and others	

Source: Chartis Research

Table 2: Assessment criteria for vendors of payment fraud solutions, 2024

Completeness of offering	Market potential
Core technology	Customer satisfaction
Fraud typologies	Market penetration
Speed, volume and performance	Growth strategy
Fraud and analytical models	Business model
Solution packaging and deployment	Financials
Payment rails	
Card payments	
Real-time payments	
Other A2A/Wire payments	
ACH fraud	
Check fraud	
Alternative payments	

Source: Chartis Research

Table 3: Vendor capabilities for enterprise fraud solutions, 2024 – core technology

Vendor	Advanced/proprietary fraud-detection techniques	Behavioral monitoring	Libraries of pre-packaged fraud rules	Modeling and testing	Solution packaging and deployment	Platform, workflow and analytics
Abrigo	***	****	****	***	*****	****
BPC	****	****	***	*****	****	****
Clari5	*****	****	*****	****	****	****
DataVisor	****	*****	****	****	****	****
Effectiv	****	****	****	*****	****	****
Feedzai	*****	*****	****	*****	****	*****
FICO	*****	****	*****	*****	****	*****
FIS	*****	****	****	*****	****	****
Focal	****	***	***	****	****	***
IDVerse	***	***	***	****	****	***
INFORM	****	****	****	****	***	****
LexisNexis Risk Solutions	****	****	****	****	****	*****
Lynx	****	*****	****	*****	****	****
Manipal Group	****	***	*****	***	***	****
Minerva	***	**	**	***	***	****
Nasdaq Verafin	****	****	****	*****	*****	****
NetGuardians	****	****	****	****	****	****
NICE Actimize	*****	*****	*****	*****	*****	****
Quantexa	*****	***	****	*****	****	*****
Refine Intelligence	****	***	**	****	****	***
Rozes	***	***	**	***	***	****
SAS	*****	****	*****	*****	****	*****
Sumsub	****	****	****	****	****	****
SymphonyAI	****	****	****	****	****	****
Tookitaki	****	****	*****	****	****	****
Veriff	****	****	***	****	****	***

Key: ***** = Best-in-class capabilities; **** = Industry-leading capabilities; *** = Advanced capabilities; ** = Meets industry requirements; * = Partial coverage/component capability

Source: Chartis Research

Table 4: Vendor capabilities for enterprise fraud solutions, 2024 – fraud typologies

Vendor	Application fraud and identity risk	APP and social engineering	Mule detection	Cyber and others
Abrigo	*	*	***	*
BPC	***	****	****	*****
Clari5	*****	*****	*****	****
DataVisor	***	****	***	****
Effectiv	****	****	****	***
Feedzai	****	*****	*****	*****
FICO	*****	*****	****	****
FIS	****	****	****	****
Focal	****	****	****	***
IDVerse	*****	*	*	****
INFORM	****	****	***	****
LexisNexis Risk Solutions	*****	****	****	*****
Lynx	**	****	*****	****
Manipal Group	****	****	***	****
Minerva	****	***	****	**
Nasdaq Verafin	*****	*****	*****	****
NetGuardians	**	*****	****	****
NICE Actimize	*****	*****	*****	****
Quantexa	****	*****	*****	***
Refine Intelligence	**	**	****	***
Rozes	****	**	***	*
SAS	****	*****	*****	****
Sumsub	*****	***	****	*****
SymphonyAI	***	****	*****	****
Tookitaki	****	*****	*****	**
Veriff	*****	***	***	****

Key: ***** = Best-in-class capabilities; **** = Industry-leading capabilities; *** = Advanced capabilities; ** = Meets industry requirements; * = Partial coverage/component capability

Source: Chartis Research

Table 5: Vendor capabilities for payment fraud solutions, 2024 – core technology

Vendor	Fraud typologies	Speed, volume and performance	Fraud and analytical models	Solution packaging and deployment
Abrigo	****	****	****	*****
BPC	****	****	*****	****
Clari5	****	*****	****	****
DataVisor	***	*****	****	****
Effectiv	****	****	*****	****
Feedzai	*****	*****	*****	****
FICO	****	*****	*****	****
FIS	****	*****	*****	****
Focal	****	***	***	***
INFORM	****	*****	****	****
LexisNexis Risk Solutions	****	*****	****	****
Lynx	****	****	*****	****
Manipal Group	****	****	****	***
Minerva	***	**	***	***
Nasdaq Verafin	*****	*****	*****	****
NetGuardians	****	*****	****	*****
NICE Actimize	*****	*****	****	*****
Refine Intelligence	***	***	****	****
Rozes	**	**	***	***
SAS	*****	*****	*****	****
SymphonyAI	****	*****	****	****
Tookitaki	****	****	****	****

Key: ***** = Best-in-class capabilities; **** = Industry-leading capabilities; *** = Advanced capabilities; ** = Meets industry requirements; * = Partial coverage/component capability

Source: Chartis Research

Table 6: Vendor capabilities for payment fraud solutions, 2024 – payment rails

Vendor	Card payments	Real-time payments	Other A2A/Wire payments	ACH fraud	Check fraud	Alternative payments
Abrigo	**	****	****	*****	*****	***
BPC	*****	****	****	***	***	****
Clari5	*****	*****	****	***	***	****
DataVisor	****	****	****	****	***	***
Effectiv	****	****	****	*****	****	****
Feedzai	*****	*****	****	****	****	*****
FICO	*****	*****	****	****	****	****
FIS	*****	*****	*****	****	***	****
Focal	***	***	***	**	*	***
INFORM	*****	*****	****	****	**	****
LexisNexis Risk Solutions	****	****	****	****	****	****
Lynx	*****	****	****	****	***	****
Manipal Group	***	***	***	**	*	***
Minerva	***	**	**	**	**	****
Nasdaq Verafin	*****	*****	****	*****	*****	*****
NetGuardians	****	****	*****	***	***	****
NICE Actimize	*****	*****	****	*****	*****	****
Refine Intelligence	**	**	**	**	*****	**
Rozes	**	**	**	**	*	***
SAS	*****	*****	*****	*****	*****	*****
SymphonyAI	**	*****	*****	****	***	***
Tookitaki	****	****	****	****	***	****

Key: ***** = Best-in-class capabilities; **** = Industry-leading capabilities; *** = Advanced capabilities; ** = Meets industry requirements; * = Partial coverage/component capability

Source: Chartis Research

1. Note that references to companies in the text of this report do not constitute endorsements of their products or services by Chartis.

Jump to top

Appendix A: RiskTech Quadrant® methodology

Chartis is a research and advisory firm that provides technology and business advice to the global risk management 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® reports are written by experienced analysts with hands-on experience of selecting, developing and implementing risk management systems for a variety of international companies in a range of industries, including banking, insurance, capital markets, energy and the public sector.

Chartis' research clients include leading financial services firms and Fortune 500 companies, leading consulting firms and risk technology vendors. The risk technology vendors that are evaluated in the RiskTech Quadrant® reports can be Chartis clients or firms with whom Chartis has no relationship. Chartis evaluates all risk technology vendors using consistent and objective criteria, regardless of whether they are a Chartis client.

Where possible, risk technology vendors are given the opportunity to correct factual errors prior to publication, but cannot influence Chartis' opinion. Risk technology vendors cannot purchase or influence positive exposure. Chartis adheres to the highest standards of governance, independence and ethics.

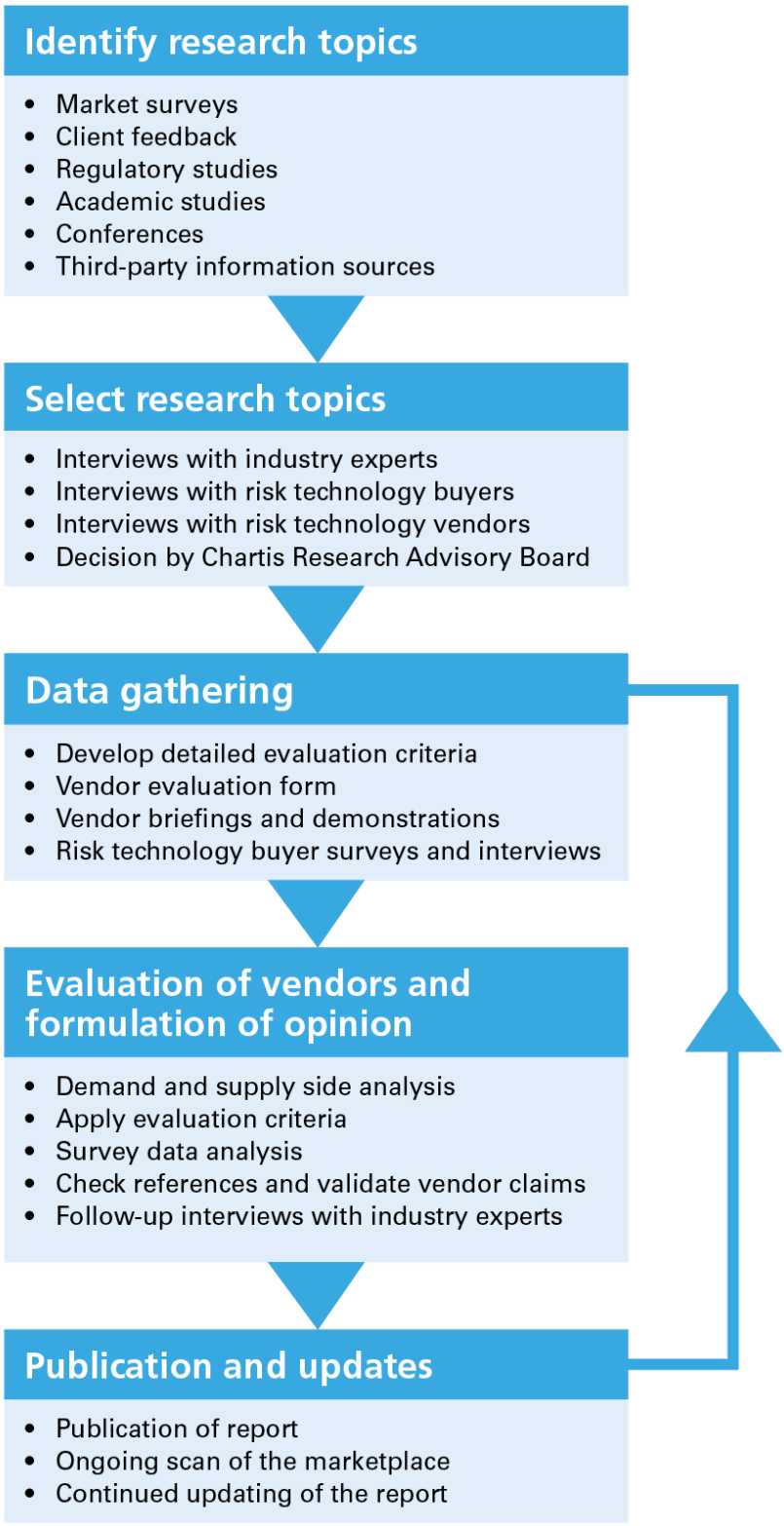
Inclusion in the RiskTech Quadrant®

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

Research process

The findings and analyses in the RiskTech Quadrant® reports reflect our analysts' considered opinions, along with research into market trends, participants, expenditure patterns and best practices. The research lifecycle usually takes several months, and the analysis is validated through several phases of independent verification. Figure 5 below describes the research process.

Figure 5: RiskTech Quadrant® research process



Source: Chartis Research

Chartis typically uses a combination of sources to gather market intelligence. These include (but are not limited to):

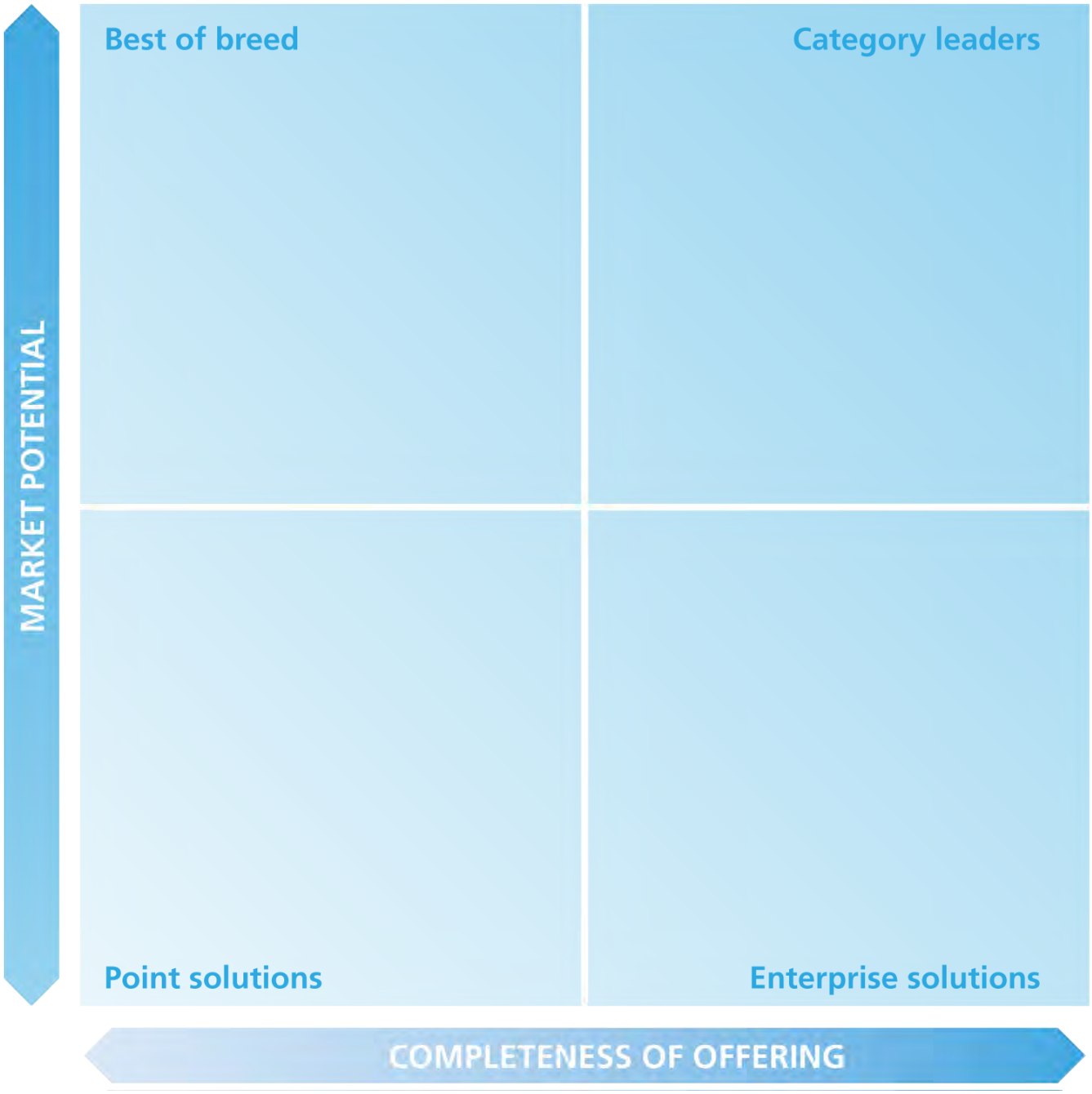
- **Chartis vendor evaluation forms.** A detailed set of questions covering functional and non-functional aspects of vendor solutions, as well as organizational and market factors. Chartis' vendor evaluation forms are based on practitioner-level expertise and input from real-life risk technology projects, implementations and requirements analysis.
- **Risk technology user surveys.** As part of its ongoing research cycle, Chartis systematically surveys risk technology users and buyers, eliciting feedback on various risk technology vendors, satisfaction levels and preferences.
- **Interviews with subject matter experts.** Once a research domain has been selected, Chartis undertakes comprehensive interviews and briefing sessions with leading industry experts, academics and consultants on the specific domain to provide deep insight into market trends, vendor solutions and evaluation criteria.
- **Customer reference checks.** These are telephone and/or email checks with named customers of selected vendors to validate strengths and weaknesses, and to assess post-sales satisfaction levels.
- **Vendor briefing sessions.** These are face-to-face and/or web-based briefings and product demonstrations by risk technology vendors. During these sessions, Chartis experts ask in-depth, challenging questions to establish the real strengths and weaknesses of each vendor.
- **Other third-party sources.** In addition to the above, Chartis uses other third-party sources of information such as conferences, academic and regulatory studies, and collaboration with leading consulting firms and industry associations.

Evaluation criteria

The RiskTech Quadrant® (see Figure 6) evaluates vendors on two key dimensions:

1. Completeness of offering
2. Market potential

Figure 6: RiskTech Quadrant®



Source: Chartis Research

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.

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 varies 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 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, 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 descriptions

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 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.

Focused functionality will often see best-of-breed providers packaged together as part of a comprehensive enterprise risk technology architecture, co-existing with other solutions.

Enterprise solutions

Enterprise solutions 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.

Category leaders 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.

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

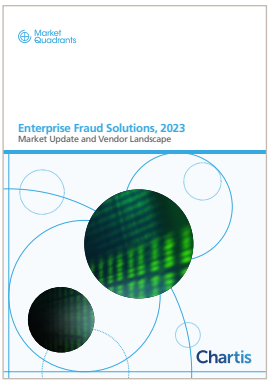
Jump to top

Copyright Infopro Digital Limited. All rights reserved.

As outlined in our terms and conditions, **https://www.infopro-digital.com/terms-and-conditions/subscriptions/** (point 2.4), printing is limited to a single copy.

If you would like to purchase additional rights please email **info@chartis-research.com**

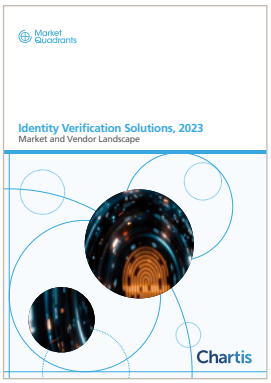
Further reading



Enterprise Fraud Solutions, 2023: Market Update and Vendor Landscape



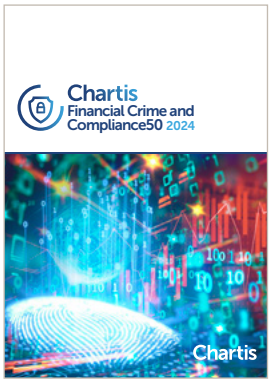
Payment Risk Solutions, 2023: Market and Vendor Landscape



Identity Verification Solutions, 2023: Market and Vendor Landscape



FRAML Solutions, 2023: Market and Vendor Landscape



Financial Crime and Compliance50 2024



RiskTech100 2024

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