Market Quadrants

Financial Crime Risk Management Systems: Enterprise Fraud

Market Update 2018

Chartis

Independent. Insightful. Actionable.

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 Waters Technology. Chartis's 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 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 including Basel 2 and 3, Dodd-Frank, MiFID II and Solvency II

Chartis is solely focused on risk and compliance technology, which gives 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 implementing and developing risk management systems and programs for Fortune 500 companies and leading consulting houses.

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

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

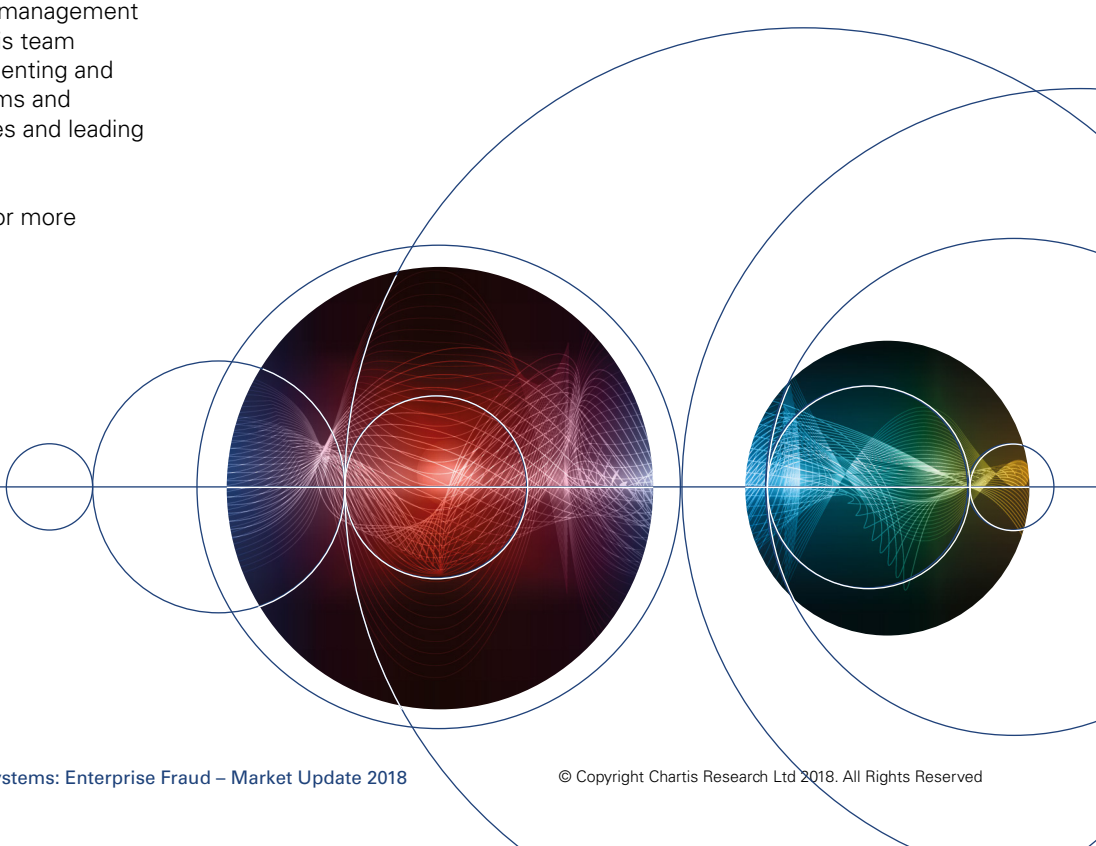


Table of contents

List of figures and tables

1. Executive summary

The anti-fraud sector remains a hotbed of risk management activity. As criminals become ever more technically proficient, Financial Institutions (FIs) find themselves in a constant 'arms race', attempting to stay one step ahead. In recent years, the main theme in anti-fraud has been diversity. A wide range of new threats (and possibilities) has emerged, as technological changes inside and outside FIs have exposed them to faster payments, risky intermediaries, and new technical environments that include cloud deployments, 'container' technologies and open Application Programming Interfaces (APIs).

Since we last analyzed this market[1], these developments have influenced several prevalent trends in enterprise fraud and the way it is managed:

- **Attempts to integrate fraud have struggled, and it remains a standalone discipline**. While anti-fraud has a number of links with cybersecurity and Anti-Money Laundering (AML), organizations have struggled to integrate their various systems. This is because of fundamental differences in the speed of response (real-time payments vs batch AML reporting, for example), risk appetites and organizational structures (fraud and AML are typically managed by separate departments with asymmetric responsibilities and budgets). And while cybersecurity is increasingly inextricable from anti-fraud – almost all fraud is now at least partially cyber-enabled – it is still often managed by separate investigative teams and technical functions. As a result, as the anti-fraud ecosystem becomes more complex, it remains a largely distinct discipline.

- **The need for speed**. Across the world, the time taken to process and clear payments is speeding up, and to respond effectively anti-fraud systems must be both fast and accurate. For FIs, the challenge is to keep pace with the rapidly increasing velocity of transactions within the constraints imposed by their infrastructure (such as their core banking processes or relational databases).

- **A focus on payments**. The payments landscape is evolving quickly; by contrast, other areas of fraud are relatively static. These areas (notably account-based fraud) have a higher burden of proof, and depend more heavily on investigations. Investigating long-term fraud activities is complex, involving the analysis of multiple factors to determine fraudulent activity. Technical and personal experience are highly valued, and incumbent technology providers are difficult to dislodge.

- **The 'open' bank**. Spurred on by digital innovation, banks are becoming more 'open', using APIs and hosted services to reach and manage their customers in new ways. This is feeding into a complex technical ecosystem with a wide variety of approaches and processes and little standardization. In turn this is creating specific 'technological niches' and new potential hiding places for fraudsters.

- **New financial providers** are emerging as payment channels evolve and become more streamlined. While these newcomers are unlikely to dislodge incumbent FIs (at least in more developed economies), they add another layer of complexity in monitoring the potential gaps between merchants, intermediaries and customers. They also require risk management and anti-fraud capabilities, which may be built into their systems or provided by vendors.

The impact of these trends on the anti-fraud marketplace is clear. As the market expands, it is becoming ever more diverse, leading to a split in the vendor landscape. Incumbent vendors, with their deep risk libraries and powerful and flexible case management systems, remain difficult to dislodge, and continue to dominate investigative and account-based fraud. The faster-moving, more flexible payments market, meanwhile, is attracting new entrants that are taking market share in areas such as payment fraud, advanced analytics and infrastructure. And as banks open up and new FIs emerge, vendors are becoming more focused, matching their offerings to APIs, core banking infrastructure and 'container' technologies used to deliver packaged applications.

Pre-existing and new vendors – even FIs themselves – will jostle for space. Whatever section of the market they cater to, vendors must increasingly be able to integrate their solutions quickly and efficiently with FIs' systems, and/or provide their own advanced technologies to process risks in real time. Finally, success will be

[1] *See the Chartis report Financial Crime Risk Management Systems: Market Update 2017.*

at least partially dictated by geography, with rapidly growing banking (and therefore Financial Crime Risk Management [FCRM]) markets – such as India – offering fertile ground for all vendor types to make their mark.

This report uses Chartis' RiskTech Quadrant® to explain the structure of the market. The RiskTech Quadrant® uses a comprehensive methodology of 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 solution as the best risk management solution; it has a sophisticated ranking methodology to explain which solutions would be best for buyers, depending on their implementation strategies.

This report covers the leading vendors of enterprise fraud solutions: ACI Worldwide, Argoscope, Ayasdi, BAE Systems, Booz Allen Hamilton, BPC, CustomerXPs, EastNets, Featurespace, FICO, FIS, Fiserv, IBM, LexisNexis Risk Solutions, Manipal Group, NetGuardians, NICE Actimize, Oracle, Pelican, Quantexa, SAS, ThetaRay and Wolters Kluwer.

2. Demand-side analysis

Introduction: a long legacy of fraud

In most FIs, fraud is usually the longest-standing risk management function. Indeed, in a fundamental way it predates FIs entirely: ever since people have traded in goods and services, others have tried to steal them. The need to manage fraud, unlike other areas of Financial Crime (FinCrime), is driven mainly by business requirements rather than regulatory compliance. Whereas FIs risk heavy fines for AML breaches, for example, fraud can mean direct financial losses. Indeed, losses through fraud will often be managed as part of an FI's risk appetite – a certain level of fraud-related loss is inevitable in almost any outward-facing financial business.

Despite its age, fraud – its perpetration and its prevention – is evolving quickly. And as fraudsters acquire new ways to dodge existing controls, FIs are learning new ways to stop them. In technology terms this is evolving into something of an 'arms race'.

Key trends and implications

In this market update, we consider four main trends that are dominating anti-fraud markets:

- The continued struggle to integrate anti-fraud systems with other areas of FCRM.
- The rapid evolution of payments.
- The emergence of the 'open' bank.
- Disruption from new types of FI.

We'll explore each of these in more detail in the following sections.

Trend 1: Despite attempts to integrate it, fraud remains a distinct discipline

In recent years we have seen moves to combine AML and anti-fraud capabilities. The reasoning is sound: these are the two largest areas of FinCrime concern for FIs – bringing them together under one system makes good business sense. In reality, however, a mixture of practical and existential challenges has prevented this.

Cybersecurity integration – slowly does it

Cybersecurity involves the protection of systems, network and data from cyber attacks. Almost all fraud is at least partially cyber-enabled – while there may be some areas (such as check fraud) which are performed without computers, these are relatively minor (and often employ technology at some stage). So far, there has been a relatively slow movement of capabilities from one area into the other. Cybersecurity capabilities in anti-fraud have been limited to vendor offerings that map solution elements (such as device identities and IP addresses) onto more traditional anti-fraud tools.

Meanwhile, there has been a convergent evolution in fraud and cybersecurity solutions. Many use similar general analytical processes (such as catching a single bad actor via networks, or scoring and behavioral analysis), but there is little explicit connection between the two. Consequently, they have broadly developed into superficially similar but essentially separate ecosystems, and there are few combined cybersecurity and anti-fraud vendors.

Chartis expects the slow creep of cybersecurity information into fraud solutions to continue, especially in the area of data relating to device identification and security. This includes device identity, malware/spyware detection, and capabilities to detect 'man-in-the-middle' attacks, repudiation, impersonation and incorrect device access. These are useful differentiators, which we expect to become more important over time.

- **Time constraints**. FIs can respond relatively quickly to fraud, especially payments fraud, whereas their response to AML breaches is typically slow by comparison. Instances of AML usually require more investigation, although the intensity of this will vary from case to case.
- **Competing departments and responsibilities**. Deciding who should take charge of a unified fraud and AML infrastructure can be a challenge. Often fraud is integrated within the retail arm of the bank, whereas AML exists in the risk department.
- **Risk appetites**. Most FIs accept some level of fraud. But they cannot accept any level of money laundering, because the risks are too high (they could face billion-dollar fines). This fundamental mismatch creates further challenges, in areas such as sequencing for risk scoring – deciding which should be scored first, for example.

As a result, AML and anti-fraud have seldom been integrated effectively – if they have, it has

generally been in small or mid-sized FIs[2]. Smaller FIs tend to have relatively simple FCRM functions, typically with a limited number of stakeholders and relatively centralized infrastructure. When they build out their FCRM, it often makes sense to do so with a more integrated focus on AML and fraud. Some larger FIs are taking steps toward integration, via incremental upgrades and an integrated case-manager view, or with Financial Intelligence Units (FIUs). But they are unlikely to have fully integrated AML and anti-fraud FCRM any time soon.

Trend 2: Rapid evolution of payments

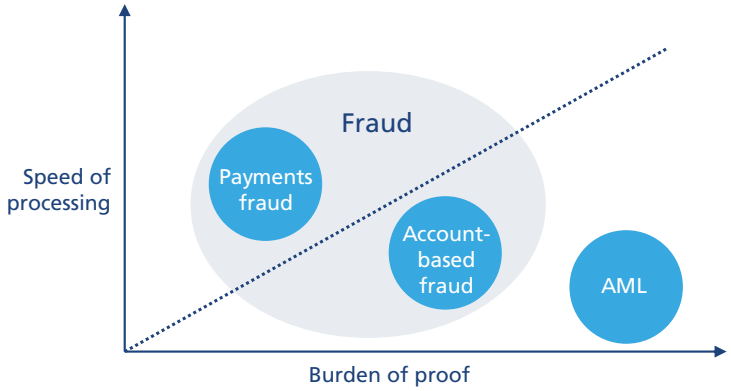
Conceptually, fraud can be subdivided in many different ways[3]. Since our last FCRM report, a notable and growing divide (from a technical and risk-management perspective) has emerged between **account-based fraud** (detecting whether the owner of an account is acting in a fraudulent way) and **payments fraud**, in which payments are falsely created or diverted. In fact, the dynamic between the two reflects the broader difference between fraud and AML discussed earlier. The key factors here are burden of proof and the speed of processing the fraud (see Figure 1).

Resolving an **account-based fraud** often involves a long and involved investigation, in which proof of fraud must be determined to a high degree of accuracy. Take 'bust-out' fraud, for example, in which the holder of a fraudulent account builds up a line of credit and then cashes out and disappears. In this case, the investigating team analyze a number of factors and processes:

- The account holder's credit history.
- The length of time the account has been active.
- The method(s) by which the account holder has interacted with the institution (via a device, for example, or in person), which affects risk scoring.
- Information about other counterparties or financial obligations.

This is a large burden of proof. And because the end result may be a criminal prosecution, human intervention is essential to ensure that the evidence collected is accurate. The same is true of many other types of account-based fraud.

Figure 1: Burden of proof and speed of processing in payments and accounts fraud and Anti-Money Laundering



Source: Chartis Research

Because of this, account-based fraud management is a well-established discipline that focuses on aiding human investigation, with an emphasis on workflow technologies (such as case management) and visualization techniques (such as heat maps and peer groupings). It relies on pre-existing knowledge of how fraudsters interact with banking systems, and well-tested and highly trusted analytics.

Conversely, the burden of proof for **payments fraud** is much lower – if fraud is detected, the payment is simply stopped or deferred. The process can be, and often is, automated. Indeed, because of the lesser burden of proof, faster response times and much larger volume of transactions, payments fraud has responded much more readily to changes in infrastructure and analytics, and to changes in the marketplace (such as the digital transformation of incumbent banks, the rise of financial intermediaries, and the growth of real-time payments).

New payment types demand new, faster analytical approaches

The speed and convenience of new payment methods has produced a surge in payment systems around the world, characterized by rapid clearing and turnaround times and easy availability on online and mobile devices (see Appendix A).

Faster payments demand faster risk management, and FIs are under pressure to monitor, match and validate the incoming and outgoing elements

[2] This lack of integration is part of the reason we have created a dedicated enterprise fraud report, to allow us to explore these fundamental challenges in more detail.
[3] Previous Chartis FCRM reports have discussed the differences between third- and first-person fraud, for example, or different types of channel-related fraud.

of transactions, which can be bank-to-bank or customer-to-customer, and which may involve intermediaries (see Figure 2). By matching incoming and outgoing transaction scores, FIs can mark them against each other and create a profile of the sender.

These new payment methods suit specific types of technology. Payment processes are often managed by high-speed streaming databases, because of high transaction volumes and low latencies, and risk scores for each transaction that are generated within milliseconds. Being able to monitor a range of channels (such as mobile phones, cards and so on) and payment types (such as Single Euro Payments Area [SEPA] and wire) is essential. In addition, because of the relatively high level of automation involved, and the low reliance on human intervention, this is an area where advanced analytics such as Machine Learning (ML) are well-established.

Ultimately this more flexible and fast-moving environment means that payments fraud presents opportunities for FIs willing to experiment with either advanced analytics (such as ML) and/or improved technical infrastructure (such as streaming databases).

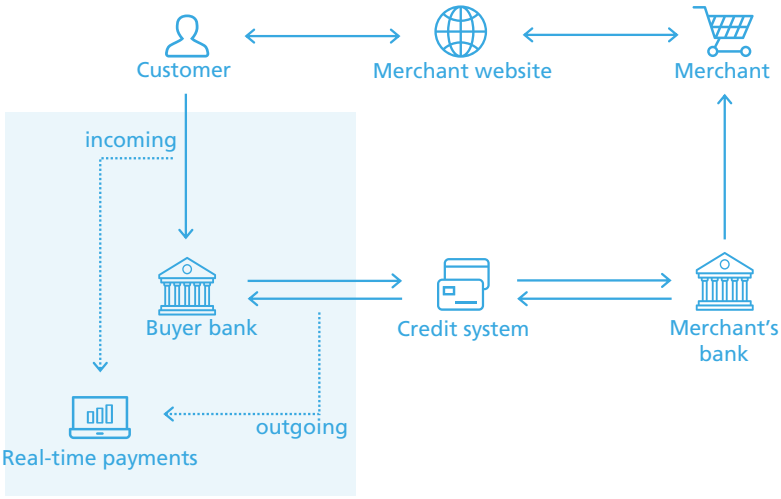
Trend 3: The 'open' bank

The surge in payments providers is due in no small part to the digital revolution in banking. Consumers' habits and expectations are changing: many now expect a fully integrated digital experience from all the organizations they interact with – banks, supermarkets, doctors, or local government offices. Partly because of this, and partly because of cost pressures, FIs have been reinventing the ways in which they manage their customers. 'Bricks and mortar' branches are losing ground to less costly and more efficient online advisory models. Increasingly, a much higher proportion of payments and accounts are managed online, creating an explosion of third-party payment providers along the value chain.

As the digital revolution takes hold, 'open' banking is becoming more prevalent, characterized by three major developments:

- **An open front end**. FIs are increasingly using APIs to allow third parties (such as payment service providers and account comparison services) to connect to them. A combination of regulatory and business pressures is responsible for this, as we explore in more detail in the next section.

Figure 2: Real-time payment gateways for a simple retail transaction



Source: Chartis Research

- **More systems on the cloud**. Concerns over cost and dealing with vast amounts of data have made cloud system deployments increasingly attractive to FIs. Hosted systems also offer FIs more flexible options for services and outsourcing, with Software as a Service (SaaS) emerging as the dominant model.

- **Core banking must be taken into account**. In terms of cost and consistency, 'ripping and replacing' core banking systems is too much of a challenge for FIs. Transformation, therefore, tends to happen at the FI's technological perimeter. However, when installing anti-fraud solutions the core banking ecosystem should not be overlooked. Pre-built or specially configured anti-fraud systems for a specific core banking architecture can provide considerable performance benefits in terms of both processing speed and speed of integration. This is significant, as many legacy institutions have infrastructure that dates back decades. The disadvantage, of course, is that any benefits will only attach to that particular core banking model.

These factors are creating an increasingly complex digital services ecosystem, and addressing it in any universal sense, and in particular with a single solution, is a challenge. The key characteristic here is variety. FIs and vendors will address the changes in different ways, determined by their institutional preferences and architectures. So far there is little standardization, nor is there much deliberation about what that might look like.

An analogy can be found in the story of US shipping containers, in which cargo was initially delivered in an array of differently shaped boxes, before the freight industry settled on standardized shipping containers). But that example was far from straightforward, and was only resolved after several years. So while Docker is currently the developers' programming language container of choice, and Amazon Web Services the most popular cloud deployment, all that could change very quickly. Flexibility remains the name of the game.

At the moment, open banking systems use programming languages like Java, Python, Docker, UberNet or COBOL for their 'containers'. These different environments are complex, and FIs have their own preferences for particular capabilities, cloud strategies and infrastructure. Meanwhile, as we have seen, underlying core banking infrastructures are a consistent determining factor in the speed of integration and processing speed for anti-fraud solutions.

Trend 4: FinTech and the new intermediaries

The story of the rise of FinTech and 'financial disintermediation' has raised the possibility of lighter-weight, agile and innovative challengers stealing market share from incumbent FIs. So far FinTechs have done little to displace banks as the central providers of risk and lending services, and instead have largely been ancillaries to the incumbents.

But being a 'first mover' in any new technology is a useful advantage. And not just for providers: fraudsters will find innovations just as tempting, using new transaction methods to conceal their intentions, or steal identities, or redirect payments.

Table 1 summarizes some of the more notable global FinTech developments in recent years.

Table 1: Key global FinTech initiatives

Country/Region	Initiative
UK/Europe	PSD2* and the Open Banking† initiative are designed to allow FinTechs to connect to banks' systems. The growth in scope from PSD1 represents a slow creep of regulation into payments and account comparisons being provided by FinTechs. Incremental, step-wise coverage across these areas will bring them steadily under the remit of government regulation.
US	Tech firms like Apple, Square and PayPal have been engaging in more 'bank-like' activity, facilitating payments, running money-market funds, and offering mobile payments and pre-paid cards. Amazon's business lending division is growing quickly, but focuses mainly on 'complementary' services through bank partnerships, rather than taking on credit risk and opening itself up to banking regulation. So far these are unregulated, and compared to banks are still a very small segment of the market. Most have intermediary or escrow functionality, rather than providing credit and lending facilities.
Africa	Mobile payments are extremely popular, so much so that many 'traditional' banking systems are being bypassed completely. Mobile money transfer systems are common (such as the M-Pesa mobile phone-based system in Kenya). That said, mobile payment systems often connect to incumbent institutions rather than new challenger banks. The African scenario, therefore, is closer to the European model than the Chinese one, albeit with more integral FinTech firms.

Country/Region	Initiative
Asia-Pacific	Several new payment companies have appeared in India, and are more 'bank-like' than other similar offerings. Most prominent among these is Paytm, which the Reserve Bank of India has declared a 'payment bank'. It is funded by Ant Financial, an arm of the Chinese company Alibaba (which is discussed in more detail below). The Chinese market is where most disintermediation has occurred. Two digital payment providers – Alibaba and Tencent – dominate, the result of a combination of government-led initiatives and a less well-established traditional banking system. Services provided include wealth management, lending, insurance and credit scoring. Alipay (Alibaba's payment service) and WeChat (Tencent's payment/chat service) together accounted for $2.9 trillion of transactions in 2016; by September 2017 they accounted for 93% of China's mobile payments market.‡ The integrated nature of these systems (including shopping and social media) means that fraud is debatably even more complex, and the risk of identity fraud even higher.

* *PSD2 is designed to regulate payment services and payment service providers throughout the European Union and European Economic Area (see* **https://ec.europa.eu/info/law/payment-services-psd-2-directive-eu-2015-2366_en***).*
† *Established by the European Banking Authority, the aim of the Open Banking Initiative is to help firms develop market services and digital identity solutions (see* **https://www.openbankingeurope.eu/***).*
‡ **https://www.tearsheet.co/payments/5-charts-on-how-mobile-payments-are-growing-in-china**
Source: Chartis Research

Recent developments in Europe could make it a test-bed for the latest anti-fraud developments. The PSD2 and Open Banking initiatives could be seen as an attempt by European governments to gain a foothold in FinTech. There are two views of this from a strategic macro-level perspective. The more cynical interpretation sees it as a possible lifeline for debt-laden European banks, giving them more ways to cross-sell and lend at higher margins. The more benign view is that the EU is attempting to establish best practices for data and financial management in an unsure environment.[4] Whatever the underlying reason (most likely a hybrid of the two), the implications for tackling fraud are worth analyzing.

One of the major developments will be the introduction of new intermediaries (such as those introduced by PSD2: Payment Initiation Service Providers [PISPs] and Payment Services Providers [PSPs]). Not only will these have to be 'risk scored' by FIs, they also create new process 'corners' (between customers and merchants) in which fraudsters can lurk (see Figure 3).

FIs will have to monitor these relationship much more closely. Each of the red arrows in Figure 3 represents an area where a fraudster can potentially intercept or change a transaction. In particular, the pathways between customer and PISP are particularly vulnerable to identity fraud.

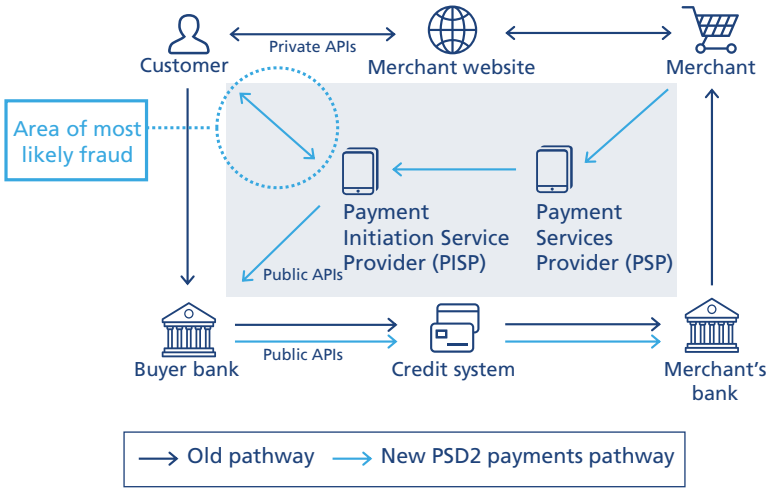
The areas that FIs will have to focus on include:

- Behavioral analysis of relationships with third parties, to monitor them against their peers and against their own historical behavior ('is this third party acting strangely?').
- Device management – determining how, where and why customers or third parties are connecting to the FI.
- Risk-scoring customers' authenticity. This uses combinations of knowledge (i.e., the passwords customers use), possessions (i.e., a mobile device ID), and inherence (biometric identification, for example). PSD2 requires at least two of these in a risk score.

[4] *There is a third view: that such moves allow governments and regulators to harness the digital revolution to create the increased competition and access they have struggled to deliver through more conventional means.*

Again, diversity is the central theme here. In this particular case, the issue is less about the technical diversity of the FI's infrastructure than the increased number of entities the FI must manage. Chartis predicts that the diversity of anti-fraud data processed will increase alongside these requirements for device information, IP addresses and biometric identification.

Figure 3: New entities and pathways mandated by PSD2



Source: Chartis Research

3. Supply-side analysis

Technology trends, implications and requirements

The growing diversity in the anti-fraud sector is creating similar diversification, splits and divisions in the corresponding vendor landscape. Four main supply-side trends have emerged, mirroring those on the demand side:

- A split in offerings for account and payment fraud.
- A focus on specific elements of the 'open bank' solution.
- The need for FinTech-focused risk management.
- The growing influence of geography.

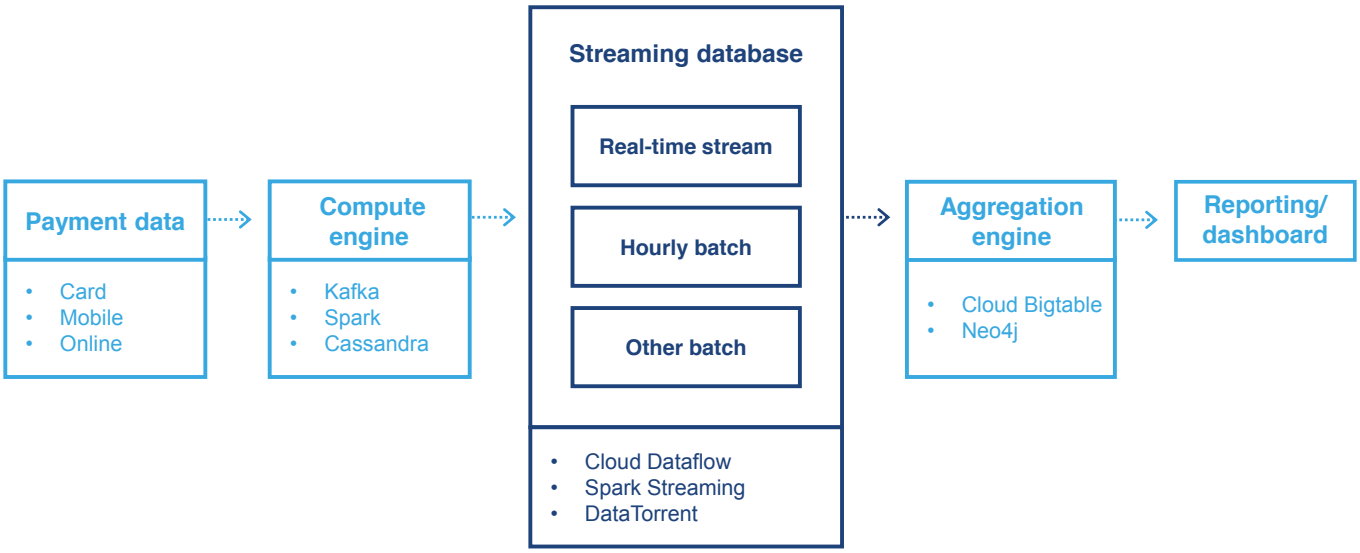
We explore these trends in more detail in the following sections, before considering the current vendor landscape and how we assessed providers for this report.

Trend 1: A split in provision – accounts versus payments

Growth in the number and speed of payments has created a split in the technology requirements for account-related fraud. The split isn't a neat one, though, and there is overlap across both sides. Dealing with **account-based fraud** requires deep experience in the more complex problems of transactional fraud, as well as large libraries of reliable fraud analytics. Flexible case management functionality enables tasks and processes to be configured, and there is even scope for Robotic Process Automation (RPA). However, because anti-fraud systems typically involve fewer Full-Time Employees (FTEs) than AML and Know Your Customer (KYC) processes, RPA is likely to prove less transformative in a fraud context.

The ability to configure, visualize and automate tasks and processes is invaluable for FIs. As we have seen, integrating cross-channel fraud and/or AML data for deep investigative capabilities (such as those provided by integrated FIUs), is rare, and likely to be provided only by the largest, most

Figure 4: A streaming architecture for payments fraud



Source: Chartis Research

experienced vendors. And because integrating the FinCrime functions of larger FIs in particular remains a significant challenge, these projects are tending to shift downmarket slightly, toward mid-size/Tier 2 FIs.

New capabilities needed

Rapid change in the **payments market** is triggering advances in both analytics (such as ML or topological data analysis) and the underlying technical infrastructure. SQL or NoSQL databases, for example, may not have the necessary read/write speed to manage what could amount to tens of thousands of transactions per second. A payments architecture should address requirements such as:

- Matching and reconciling real-time and batch data processing. This is one of the key requirements of payment monitoring. Systems will have to provide real-time (or near real-time) responses to data without affecting the underlying information. This could include reading back into a larger data lake or external information repository, or even matching the behavior of an entity to its history.
- Ensuring resilience and fast recovery from failure.
- Offering the flexibility to support varied analytics processes.
- Time-stamping and documenting events, to enable review and audit.
- Providing scalability and flexibility to account for surging account volumes.

To summarize what might be required, Figure 4 illustrates some of the capabilities of a real-time streaming infrastructure, including the potential components (Kafka, Spark, etc.) that a vendor (or institution) may utilize.

Trend 2: The open bank – picking the right technology for the right problem

As the ecosystem around 'open' banks develops, matching FIs' needs with vendors' offerings will be vital. **FIs and vendors must address five major areas** within the banking framework:

- **Streaming data architecture** (discussed above in more detail).
- **Cloud services**, to host fraud and model risk management solutions. Increasingly, FIs have been using SaaS solutions for fraud and FinCrime.
- **Container analytics**. These deliver analytics with an entire runtime environment – an application, all its dependencies, libraries and other binaries, and the configuration files needed to run it – bundled into one package. FIs like them because they do not require specialized operating systems, and they consume less power than other options.
- **Data lakes**. Many firms increasingly use data lakes – traditionally high-volume NoSQL or Hadoop data stores – as centralized repositories for multi-channel fraud, or even to store AML and fraud data.
- **Legacy data stores and core banking**. FIs often build their own core banking systems – frequently pre-Internet-era systems designed for nine-to-five branch banking.

Vendors should – and many do – devise a strategy and toolkit for each of these areas (as outlined in Figure 5). If they don't provide streaming databases or cloud solutions, for example, they may choose to provide APIs that can link to third-party or core banking services.

One key differentiating factor is the *analytical* flexibility of the solution. A number of vendors include capabilities to monitor, benchmark and edit fraud models and rules. Large/Tier 1 firms in particular, which tend to have more experienced staff, may wish to write their own models to account for the complexity of their business. Some vendors now enable FIs to build in languages such as R, Python and SQL, and provide APIs for running third-party models within the FIs' own systems.

Trend 3: 'Disruptive' FinTechs still need risk management

The FinTechs entering the financial services and banking ecosystem – whether they connect to existing institutions via APIs or provide their own services – should be managed and risk-scored. Intermediaries new and old can be scored effectively with behavioral modeling, device management and authentication tools. Increasingly, vendors now also provide systems to the new challengers more directly, either through sales or via partnerships, as new entrants look to incorporate anti-fraud tools into their own core

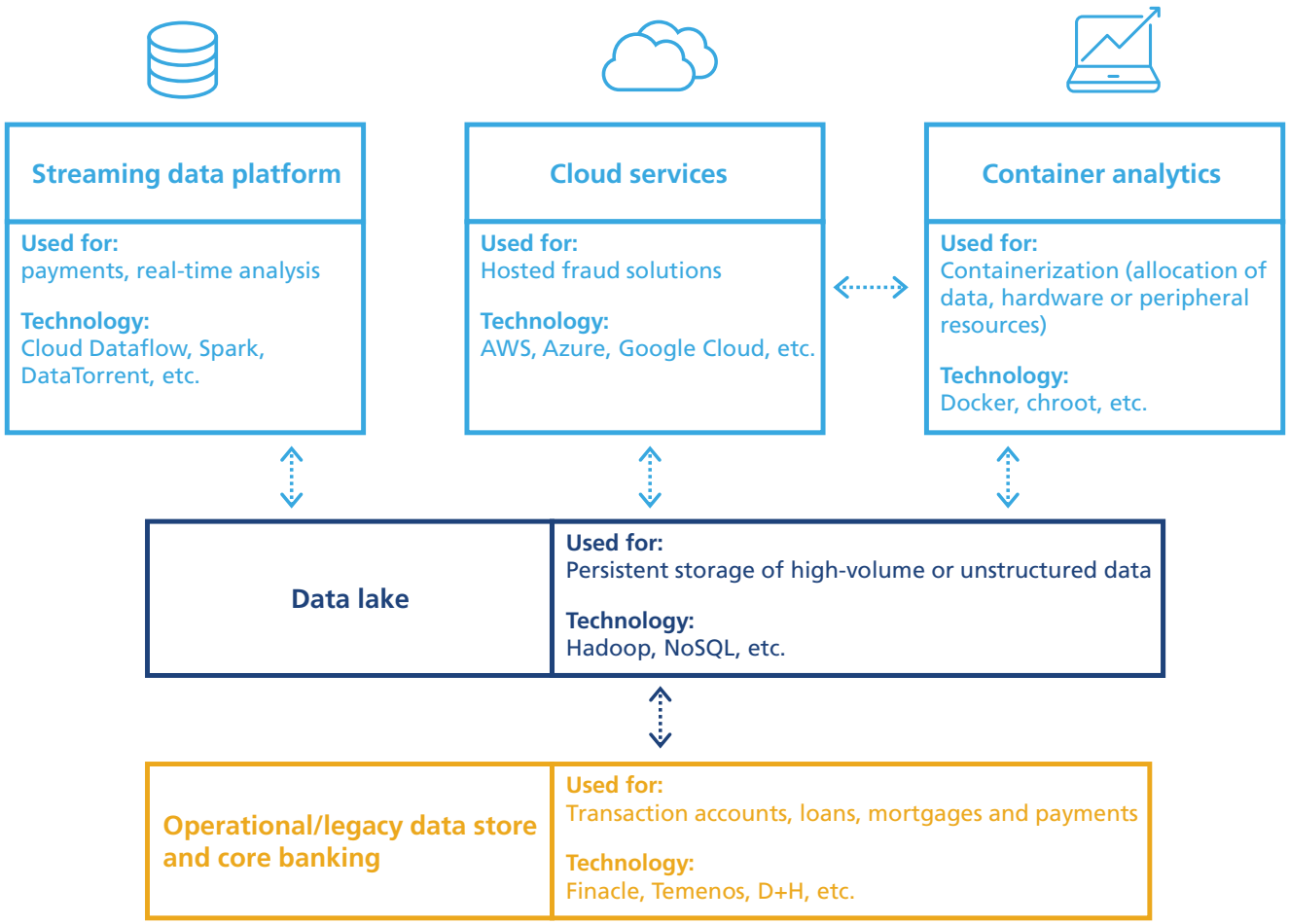
systems. In contrast to previous approaches, in which core banking systems had to layer on anti-fraud capabilities after installation, many FinTechs understand that they should have FCRM capabilities – covering sanctions and adverse media, for example, and anti-fraud analytics – built in as early as possible. PayPal, for example, recently bought anti-fraud provider Simility[5] to add in-built anti-fraud capabilities to its merchant platform.

Indeed, we might expect FinTechs to have an obvious answer to the perennial 'buy or build' question. Rather than paying license fees to outsiders, it presumably makes more sense to incorporate anti-fraud capabilities from the start, particularly as there is so much inexpensive and/or open-source technology available. However, many FinTechs are focused on keeping their processes as lean and agile as possible, in an attempt to hit performance benchmarks and provide constant updates to customers. For many, implementing financial crime and fraud systems at the same time will be too much of a challenge. Because they will be looking to outside vendors to help, FinTechs – from payment providers to cryptocurrency exchanges to insurance technology providers – represent a large potential market. A number of bespoke vendors have already emerged to address these specific firms.

Trend 4: Global differences remain significant

Several vendors in the enterprise fraud landscape have a global reach, but typically organizations tend to separate out by territory. To some extent this is

Figure 5: Technology strategies for the 'open' bank



Source: Chartis Research

[5] **https://www.bankingtech.com/2018/06/paypal-gets-anti-fraud-ability-with-120m-acquisition-of-simility/**

because of underlying regional trends. In Europe, a number of large universal banks cover broad swathes of the financial marketplace, including commercial and investment banking, financial services and insurance. These banks are complex enough to accommodate multiple vendors, and tend to be serviced by a group of larger European providers.

In the US, by contrast, FIs are less complex, with more clearly defined commercial and investment arms, and as a result have fewer vendors per institution. Large service bureaus also provide capabilities to the small regional US banks.

In recent years one rapidly growing marketplace has been India. A government-led initiative to onboard large sections of the population into banking accounts has created a fertile marketplace in which vendors can sell solutions to banks that require extensive, automated anti-fraud solutions. It has also led to notable growth in the domestic Indian anti-fraud market, both in terms of new vendors and expenditure in the space – not least because of the Punjab National Bank fraud,[6] one of the the highest-profile and most expensive fraud case in recent years.

Vendor landscape

Vendors of enterprise fraud risk management solutions can be characterized according to several specific approaches (see Table 2).

[6] **https://www.reuters.com/article/us-punjab-natl-bank-fraud-timeline/developments-in-the-2-billion-punjab-national-bank-fraud-case-idUSKCN1GK15U**

Table 2: A summary of enterprise fraud vendors

Type of vendor	Description
Incumbent enterprise fraud solution vendors	• Possess deep libraries of anti-fraud capabilities, in both payment- and account-based fraud. • Often constrained by aging infrastructure, but have deep experience and anti-fraud libraries. • Differentiated by their case-management capabilities and their ability to combine flexible workflow and analytics. • Will typically have started in a specific area of FCRM (such as card or account-based fraud, or even AML), and will have gradually expanded into more wide-ranging FCRM or anti-fraud capabilities. • Typically target larger FIs, with high-value and low-volume implementations, although several of these vendors now offer packaged anti-fraud solutions aimed at Tier 2 FIs and below.
New entrants	• Entered the fraud risk management space with advanced analytics and/or infrastructure capabilities (such as streaming databases for payments fraud, or graph analytics). • Often have best-of-breed capabilities for specific problems, but may be weak (or have no capabilities at all) in other areas, such as case management. • Will therefore often be employed alongside other vendors, frequently plugging into their case-management systems. • Cloud and hosted deployment models are common, and modular systems and APIs are essential for connecting to other areas of the risk technology stack.
Core banking integrators	• Numerous vendors have been integrating more closely with core banking systems (typically those designed within the last 10 years). • This has advantages and drawbacks. ◦ It enables quick deployment and time-to-value for the corresponding core banking infrastructure. In essence, the fraud solution is designed to fit effectively into the core banking infrastructure – much like a key in a lock. ◦ It also constrains the vendor toward that specific core banking infrastructure, giving these firms a relatively small but more approachable target market. Regional trends can contribute to this.* • Typically integrations are pre-built when systems are designed, although some firms have developed closer relationships with core banking vendors to cross-sell to their clients.
Cross-over providers	• FCRM in general, and anti-fraud in particular, has long received input from the military and/or intelligence community. Vendors continue to move across from these areas to apply analytics and services to anti-fraud systems. These firms typically employ proprietary analytics and/or a strong services arm, with a firm base in open-source infrastructure.
Payment specialists	• Similar to new entrants, payment specialist firms tend to use advanced architectures (normally streaming databases) to enhance process speeds at high volumes and low latencies. They have advantages over new entrants in their greater experience and wider libraries, but may have heavier infrastructure and longer implementation times.

* *Following the Punjab National Bank fraud, for example, Indian banks were ordered to integrate their core banking systems with SWIFT to ensure that no transaction messages, loans or guarantees were sent without being reflected in core banking or accounting systems (see* **https://uk.reuters.com/article/us-punjab-natl-bank-fraud-swift-exclusiv/exclusive-indias-pnb-adopts-strict-swift-controls-after-mega-fraud-case-idUKKCN1G52LQ***).*

Source: Chartis Research

RiskTech Quadrant® for enterprise fraud solutions, 2018

Figure 6 describes Chartis' view of the vendor landscape for enterprise fraud solutions. The RiskTech Quadrant® is a proprietary methodology developed specifically for the risk technology marketplace. It takes into account the product and technology capabilities of vendors, as well as their organizational capabilities.

Table 3 rates the specific capabilities of the vendors.

Appendix C sets out the generic methodology and criteria used for the RiskTech Quadrant®. Specifically, we have considered the following criteria as particularly important:

Completeness of offering:

- **Payment fraud**, including card, mobile and wire payment capabilities.
- **Internal fraud analytics**, including employee fraud.
- **Real-time detection capabilities**, with a focus on processing latencies and transactions per second.
- **Fraud detection techniques**, including account-based fraud, visualizations and analytics.
- **Libraries of pre-packaged fraud rules**, including specific pre-packaged rules for the fraud types included in Appendix B.
- **Alert management**, including case management and workflow.

Market potential:

- **Customer satisfaction**, including references and case studies.
- **Market penetration**, including geographical and vertical (investment, retail) clients.
- **Growth strategy**, including recent expansion, targeted areas, and roadmap.
- **Financials**, including deal size, number of clients, and the financial strength of the company.

Figure 6: RiskTech Quadrant® for enterprise fraud technology solutions, 2018

** RELX Group acquired ThreatMetrix in early 2018 and incorporated it into LexisNexis Risk Solutions.*
Source: Chartis Research

Table 3: Vendor capabilities for enterprise fraud technology solutions, 2018

	Payment fraud	Internal fraud analytics	Real-time detection capabilities	Fraud detection techniques	Libraries of pre-packaged fraud rules	Alert management
ACI Worldwide	***	*	***	**	*	*
Argoscope	**	*	*	*	**	*
Ayasdi	**	**	*	***	*	*
BAE Systems	**	***	*	**	***	**
Booz Allen Hamilton	**	*	**	**	*	***
BPC	**	*	**	***	*	*
CustomerXPs	**	*	***	**	**	**
EastNets	**	**	**	*	*	*
Featurespace	***	**	**	**	*	**
FICO	***	**	**	***	**	**
FIS	**	**	**	**	**	**
Fiserv	**	**	*	**	**	**
IBM	***	**	***	**	*	*
LexisNexis Risk Solutions†	**	*	***	**	**	**
Manipal Group	**	**	**	*	**	**
NetGuardians	**	**	*	**	**	**
NICE Actimize	**	**	**	**	**	***
Oracle	**	**	**	***	**	**
Pelican	**	*	*	**	*	*
Quantexa	**	**	**	**	**	*
SAS	**	**	**	**	***	**
ThetaRay	*	**	**	**	*	*
Wolters Kluwer	*	*	*	*	*	**

† *RELX Group acquired ThreatMetrix in early 2018 and incorporated it into LexisNexis Risk Solutions.*
*Key: *** = Core strength/advanced capabilities; ** = Meets industry requirements; * = Partial coverage/component capability.*
Source: Chartis Research

Conclusion: diversity and diversification

Fraud is becoming more diverse, and vendors are branching out in response. Whereas incumbent vendors remain firmly lodged in more established types of fraud – such as account fraud – new entrants are making progress in payments fraud, with advanced analytics and innovative infrastructure.

Overarching, definitive enterprise fraud solutions are rare, so buyers should carefully match their requirements to what's available. If they require deep investigative capabilities, they are best served by enterprise vendors. More specific requirements may be best met by employing vendors that focus on specific capabilities – perhaps they can add graph analytics or entity resolution, for example, or topographical data modeling.

FIs should also determine how fraud management solutions fit with their overall technology strategy, including their cloud and container preferences or their core banking solution. Performance metrics will be particularly important in payments fraud – solutions must be able to process high payment volumes at a low enough latency. Benchmarking and results processing for automated analytics are also favored, because automation is necessary at such high speeds and volumes. Being able to test and score how these analytics function under a number of different constraints is also important.

Diversification aside, growth in demand for anti-fraud solutions is unlikely to slow, not least because of fraud's lengthy legacy. New elements added onto technical ecosystems will provide more niches for fraudsters to hide in and attack, using the very latest technological advances. ML, for example, is traditionally viewed from the perspective of *combating* fraud, but it is naïve to presume that fraudsters will not also use it to *commit* fraud. In one hypothetical situation, Artificial Intelligence (AI) could be used to learn handwriting, speech and vocal patterns in order to commit identity fraud. The information used to identify individuals will shift accordingly, and FIs will increasingly require validation from a number of different perspectives to ensure that someone is who they say they are. Ancillary data stores (such as device identities, news, and social media) will therefore become more valuable to institutions and hackers as potential caches of usable information.

Whether FinTech firms represent passing fads, stable intermediaries or the future of the financial services industry, they will have risks that must be managed. Their relationships with pre-existing institutions and industries should be managed from a risk perspective, and their own systems will increasingly require sanctions monitoring, KYC and AML processes as they come under the regulatory umbrella. Emerging markets will continue to onboard customers at a high rate, and payments will continue to get faster, while the technical infrastructure around banks will continue to transform in multiple ways.

Fraud is (and will continue to be) a test-bed for advanced analytics, including ML, as well as the transformation of infrastructure, including streaming databases and hardware acceleration. Fraudsters' adversarial nature means that the efficacy of these capabilities is often quickly and mercilessly tested. Anti-fraud remains a rapidly expanding technological jungle of risk and opportunity, with little room for error.

4. Appendix A: New payment systems around the world

Figure 7 and Table 4 outline some of the more notable examples of new payment systems.

By the end of 2018, Belgium, Slovenia, Spain, Portugal, the Democratic Republic of Congo, Hong Kong and Malaysia will have launched their own national real-time payment schemes.

While the relative maturity of new schemes varies, the drive toward faster payments is clearly near-universal.

Figure 7: Global distribution of new payment systems

Source: Chartis Research

Table 4: Selected new payment systems (numbers in brackets correspond to those in Figure 7)

Key payment models	Where?	Speed of payments	What's involved?
Faster Payments Service (2008-18); LINK; BACS; CHAPS.	UK (1)	Same-day processing	The Faster Payments Service – which offers same-day service for transactions under £250k – now processes most retail transactions. Other payment systems (such as BACS and CHAPS) are only used for large (£250k+) or batch payments.
Real-Time Payments System (RTP); launched in 2017.	US (2)	Same-day processing	Transactions are passed through the Automated Clearing House (ACH), which connects banks and credit unions. This has historically been batch-based, with a daily processing window between counterparties. Same-day payments were authorized by the National Automated Clearing House Association in 2016. These require funds to be made available to payees by the end of business on the same day.
Immediate Payment Service (IMPS); launched in 2010	India (3)	Same-day processing (via mobile devices)	IMPS – operated via HSBC – was implemented in 2010 and has gradually expanded in scope.
SWIFT; Global Payments Innovation Initiative for cross-border payments; WeChat; Alipay.	China (4)	A varied ecosystem with little homogeneity	China has a diffuse system in which local clearing houses or local banks process payments at a variety of rates. Some areas have two daily processing windows, while some have only one. WeChat and Alipay offer Internet payments through escrow systems but do not have direct payment rails.

Key payment models	Where?	Speed of payments	What's involved?
M-Pesa; South African Payments System; East African Payments System.	Africa (5)	A varied ecosystem	Africa retains a number of geographically distinct payment models, including the South African and East African Payments systems. Many variants – like M-Pesa in Kenya – have moved straight to mobile money transfers.
SEPA;TARGET Instant Payment Settlement (TIPS).	Some European countries (6)	Real-time payments; partially rolled out	As of November 2017 the SEPA Instant Payment Scheme enables transfers of up to 10,000 Euros, but it is not yet live in all European countries. TIPS will be live in November 2018.

Source: Chartis Research

5. Appendix B: Glossary

Types of fraud

- **Account takeover**. Pretending to be an existing client, a fraudster takes control of a legitimate client's account to remove funds from the account, or to use the account to deposit fraudulent items.
- **Counterfeit fraud**. A fraudster creates false items (such as antiques or paintings), and passes them off as legitimate to sell them or to obtain credit.
- **Defalcation/Internal fraud**. Employees use their position within an FI to commit fraud.
- **'Friendly' fraud**. Friends or relatives take debit cards or other methods of payment and withdraw funds without the account holder's knowledge or consent.
- **Kiting**. A fraudster deliberately moves funds between two or more accounts to disguise a lack of funds.
- **Phishing/spoofing**. A fraudster attempts to learn information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication. Normally used in conjunction with cyber-attacks.
- **Purchase fraud**. A fraudster approaches a merchant and proposes a business transaction, then uses fraudulent means to pay for it, such as a stolen or fake credit card.
- **Recruitment fraud**. A fraudster offers fictitious job opportunities that require respondents to provide personal information or payments to progress false applications.
- **Skimming**. Fraudsters obtain PIN or magnetic strip information from credit or debit cards.
- **Sleeper/Bust-out fraud**. Fraudsters establish themselves as engaged and trustworthy customers, setting up multiple accounts at the same FI, and often cycling cash between various fraudulent accounts. When a sufficiently high level of credit is obtained, the fraudsters rapidly increase their spending. This is often organized among multiple account holders.
- **Spring-boarding**. Fraudsters are added as co-signers to accounts, with or without the co-operation of the account holder.
- **True-name fraud**. A fraudster assumes another individual's identity to establish accounts and credit against his or her name and credit history.
- **Worthless deposit**. A fraudster deposits an item that will not be cleared (such as a counterfeit check) to withdraw money against funds in the account.

Types/sources of cyber-attack

- **Cyber trespass/Hacking**. Using a computer and network to steal information or money.
- **Denial of Service (DoS)**. An attempt to make a networked financial resource unavailable to its intended users, either temporarily or indefinitely, by consuming computational resources, disrupting configuration information or network components, or obstructing communication media. Often this is performed by more than one attacker, and is referred to as a Distributed Denial of Service (DDoS). FIs often regard the reputational damage and loss of customer confidence that can result from successful DoS attacks as more significant than financial losses.
- **Electronic bulletin boards**. Used for the sale of stolen identities or other potentially sensitive information.
- **Information brokers**. Individuals or brokerages that sell personal or corporate information.
- **Phishing and pharming**. Using false/counterfeit e-mails to scam users into surrendering private information.
- **Spoofing**. Sending a message from a fraudulent email address that is masquerading as another, legitimate address.
- **Spyware**. Software that gathers and removes confidential information from any computer without the knowledge of the owner.
- **Trojan horses**. Concealed code that can be disguised as a game, an e-mail attachment, or even a web page. As soon as victims run or open the application, the code installs itself on their hard drive, and then runs each time the

computer is started. One of the most popular Trojan horses is the so-called 'man-in-the-middle' or 'man-in-the-browser' attack, This is installed on a victim's computer and modifies his or her Web transactions as they occur in real time. It can then record security information (such as passwords), or alter transaction destinations without revealing this to either party.

6. Appendix C: 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's 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's 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 or not 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's opinion. Risk technology vendors cannot purchase or influence positive exposure. Chartis adheres to the highest standards of governance, independence, and ethics.

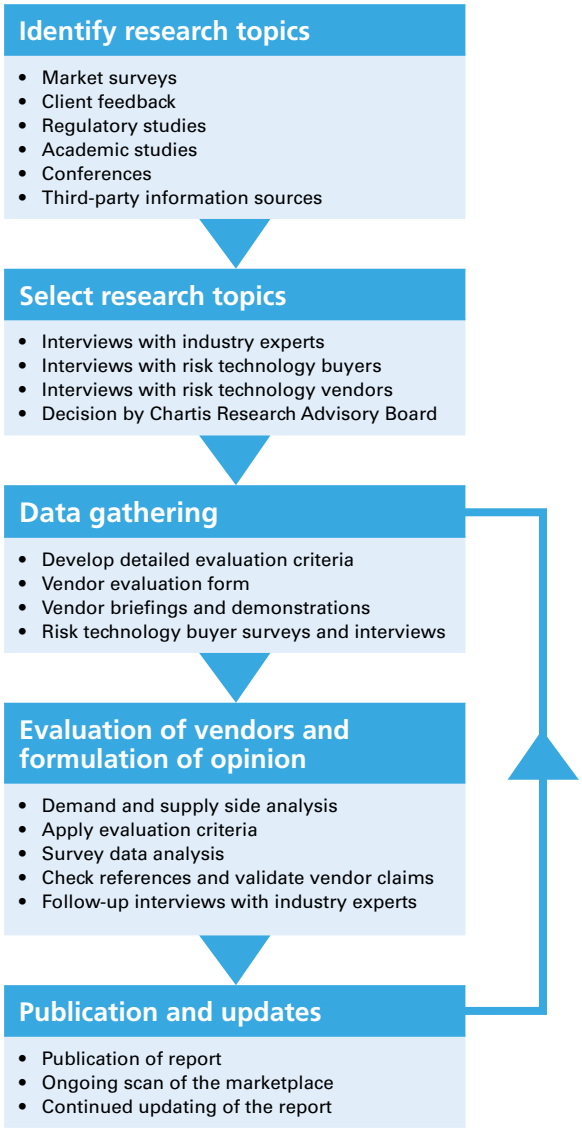
Inclusion in the RiskTech Quadrant®

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 8 below describes the research process.

Figure 8: 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's 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.

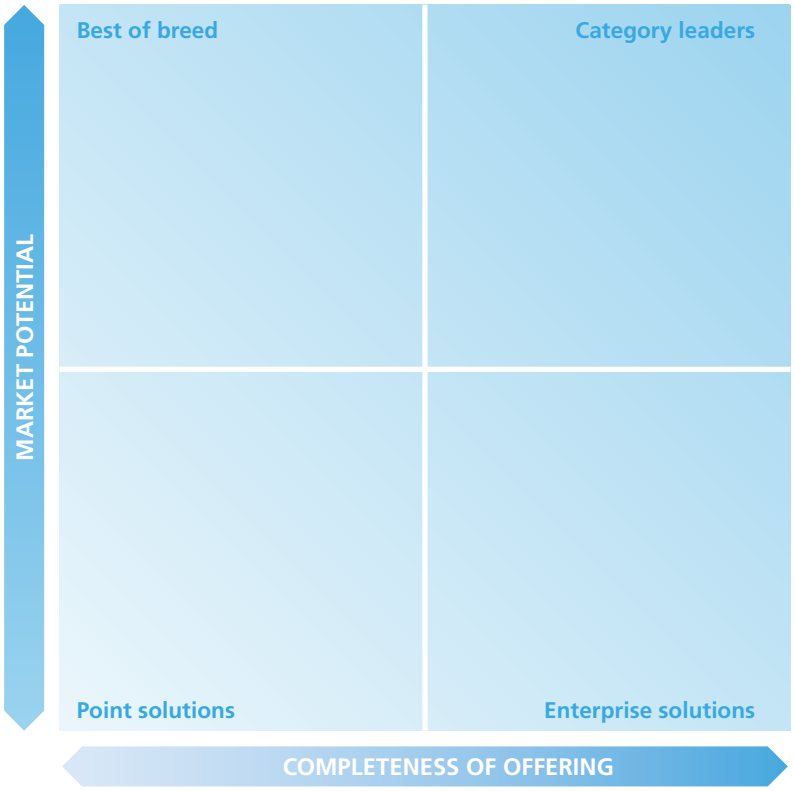
Evaluation criteria

The RiskTech Quadrant® (see Figure 9) evaluates vendors on two key dimensions:

1. Completeness of offering

2. Market potential

Figure 9: RiskTech Quadrant®



Source: Chartis Research

The generic evaluation criteria for each dimension are set out below. In addition to these generic criteria, Chartis utilizes domain-specific criteria relevant to each individual risk, which are available on request. This ensures total transparency in our methodology and allows readers to fully appreciate the rationale for our analysis.

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, 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

- **Market penetration.** Both volume (i.e. number of customers) and value (i.e. average deal size) are considered important. Also, rates of growth relative to sector growth rates are evaluated.

- **Brand.** Brand awareness, reputation, and the ability to leverage current market position to expand horizontally (with new offerings) or vertically (into new sectors) are evaluated.

- **Momentum.** Performance over the previous 12 months is evaluated, including financial performance, new product releases, quantity and quality of contract wins, and market expansion moves.

- **Innovation.** New ideas, functionality, and technologies to solve specific risk management problems are evaluated. Developing new products is only the first step in generating success. Speed to market, positioning, and translation into incremental revenues are critical success factors for exploitation of the new product. Chartis also evaluates business model or organizational innovation (i.e. not just product innovation).

- **Customer satisfaction.** Feedback from customers 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) is evaluated.

- **Sales execution.** The size and quality of sales force, sales distribution channels, global presence, focus on risk management, messaging, and positioning are all important factors.

- **Implementation and support.** 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.

- **Thought-leadership.** Business insight and understanding, new thinking, formulation and execution of best practices, and intellectual rigor are considered important by end users.

- **Financial strength and stability.** Revenue growth, profitability, sustainability, and financial backing (e.g. the ratio of license to consulting revenues) is considered as key to scalability of the business model for risk technology vendors.

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.

7. How to use research and services from Chartis

In addition to our flagship industry reports, Chartis also offers customized information and consulting services. Our in-depth knowledge of the risk technology market and best practice allows us to provide high-quality and cost-effective advice to our clients. If you found this report informative and useful, you may be interested in the following services from Chartis.

For risk technology buyers

If you are purchasing risk management software, Chartis's vendor selection service is designed to help you find the most appropriate risk technology solution for your needs.

We monitor the market to identify the strengths and weaknesses of the different risk technology solutions, and track the post-sales performance of companies selling and implementing these systems. Our market intelligence includes key decision criteria such as TCO (total cost of ownership) comparisons and customer satisfaction ratings.

Our research and advisory services cover a range of risk and compliance management topics such as credit risk, market risk, operational risk, GRC, financial crime, liquidity risk, asset and liability management, collateral management, regulatory compliance, risk data aggregation, risk analytics and risk BI.

Our vendor selection services include:

- Buy vs. build decision support
- Business and functional requirements gathering
- Identification of suitable risk and compliance implementation partners
- Review of vendor proposals
- Assessment of vendor presentations and demonstrations
- Definition and execution of Proof-of-Concept (PoC) projects
- Due diligence activities.

For risk technology vendors

Strategy

Chartis can provide specific strategy advice for risk technology vendors and innovators, with a special focus on growth strategy, product direction, go-to-market plans, and more. Some of our specific offerings include:

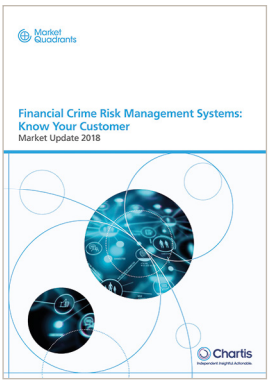
- Market analysis, including market segmentation, market demands, buyer needs, and competitive forces
- Strategy sessions focused on aligning product and company direction based upon analyst data, research, and market intelligence
- Advice on go-to-market positioning, messaging, and lead generation
- Advice on pricing strategy, alliance strategy, and licensing/pricing models

Thought leadership

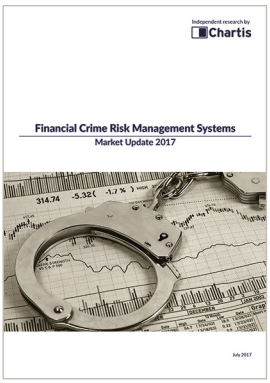
Risk technology vendors can also engage Chartis to provide thought leadership on industry trends in the form of in-person speeches and webinars, as well as custom research and thought-leadership reports. Target audiences and objectives range from internal teams to customer and user conferences. Some recent examples include:

- Participation on a 'Panel of Experts' at a global user conference for a leading Global ERM (Enterprise Risk Management) software vendor
- Custom research and thought-leadership paper on Basel 3 and implications for risk technology.
- Webinar on Financial Crime Risk Management
- Internal education of sales team on key regulatory and business trends and engaging C-level decision makers

8. Further reading

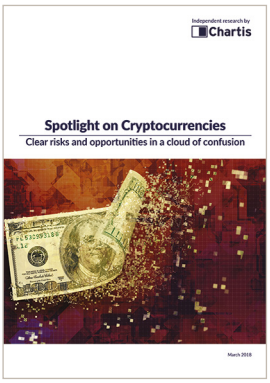


Financial Crime Risk Management Systems: Know Your Customer; Market Update 2018



Financial Crime Risk Management Systems; Market Update 2017

RiskTech100® 2018



Spotlight on Cryptocurrencies

Spotlight: quantifying cyber risk in financial institutions

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