SPARK Matrix™

Security & Risk Management

SPARK Matrix™: Enterprise Fraud Management, 2021

Market Insights, Competitive Evaluation, and Vendor Rankings

September 2021

Table of Contents

Executive Overview

This research service includes a detailed analysis of the global enterprise fraud management (EFM) market dynamics, major trends, vendor landscape, and competitive positioning analysis. The study provides competition analysis and ranking of the leading EFM vendors in the form of SPARK Matrix. This research provides strategic information for technology vendors to better understand the market supporting their growth strategies and for users to evaluate different vendors capabilities, competitive differentiation, and its market position.

Key Research Findings

Followings are the key research findings:

Technology Trends

EFM vendors are utilizing emerging technologies like automation, machine learning (ML), artificial intelligence (AI), and advanced analytics to enhance productivity, efficiency and optimize the use of valuable resources. These technologies aid organizations in spotting anomalies and lower the risks. Vendors are consistently leveraging AI, ML, automation, and advanced analytics to offer real-time monitoring and evaluation of extensive data feeds, fine-tuning risk models to accommodate new intelligence, and precise determination of risk scores for users and transactions. Moreover, vendors are ensuring seamless and safe access by utilizing various biometric authentication techniques. With the emergence of self-aware platforms integrating humans, data, and technologies, the next generation of risk management solutions is more likely to be backed by these sophisticated technologies.

Key Market Drivers Trends:

- The market drivers for the growth of EFM solutions include the growing frequency, sophistication, and complexity of fraud & cybersecurity attacks that are significantly expanding the organizations' risk exposure and the continued disruption in the technology landscape, which is driving emerging business models and leading to the wave of emerging fraud trends.

- The market drivers also include continued investments in digital transformation projects leading to increased online availability across verticals, increase in remote working, increased use of mobile and personal devices, and pandemic-related increase in online fraud. All these factors are driving the need for efficient fraud prevention solutions that offer a seamless customer experience.

- Furthermore, the global regulations and compliance requirements are increasingly becoming stringent, and there is growing scrutiny by regulators on model governance and transparency.

- Driven by the growing demand for EFM solutions to overcome frauds, including account takeover, customer abuse, loyalty abuse, card-not-present fraud, return abuse, payment fraud, cybersecurity breaches, internal fraud, and bot attacks, vendors are increasingly replacing rule-based and traditional ML-based fraud detection systems with advanced fraud management solutions. Organizations are increasingly evaluating vendors offering advanced fraud detection solutions with greater emphasis on model performance as the increasing number of fraud attacks require a flexible, scalable, and advanced EFM solution.

- Leading vendors are increasingly leveraging consortium-based shared intelligence to amplify the effectiveness of fraud models in combating the most advanced and emerging frauds. An industry consortium network enables trusted cross-industry peers to share data about shared risks for various use cases.

- With disrupted business scenarios, increase in remote working, and rise in online activity and frauds, a robust fraud management mechanism is the need of the hour in this time of the COVID-19 pandemic. Critical investments in EFM solutions are postulated to grow, with organizations focusing more on security and hassle-free user experience being the new long-term strategy to retain customers for the long term.

- The key value proposition of the EFM solution includes providing robust data integration, behavioral analytics, risk scoring, real-time fraud detection, alert and case management, self-service environment, omnichannel functionality, and visualization and reporting. The continuous transformation of EFM solutions driven by advanced technologies is propelling the market adoption amongst small to medium organizations and in large enterprises.

Competition Dynamics & Trends:

- This study includes an analysis of key vendors, including ACI Worldwide, BAE Systems, BPC, Clari5, DataVisor, EastNets, Featurespace, Feedzai, FICO, Fiserv, IBM, LexisNexis Risk Solutions, NICE Actimize, Quantexa, and SAS.

- NICE Actimize, IBM, SAS, Feedzai, ACI Worldwide, Featurespace, BPC, Eastnets and DataVisor are the top performers in the global EFM market and have been positioned as the top technology leaders in the 2021 SPARK Matrix analysis of the EFM market.

Market Overview and Technology Trends

Quadrant Knowledge Solutions defines Enterprise Fraud Management (EFM) as:

" A software that provides comprehensive real-time risk monitoring and analysis of all the transactions and application of controls for identifying internal and external fraud across all users, accounts, and channels. It provides a comprehensive analysis of the user behavior between related accounts and users across channels to help organizations identify malicious behavior, including misuse, criminal activities, compliance violations, and corruption. Thus, enterprise fraud management systems help organizations in combating risks, minimizing losses, ensuring regulatory compliance, and optimizing operational efficiencies across the organization and entities."

Global payment dynamics are rapidly changing with the growing popularity of digital banking, and emerging payment methods (mobile apps, blockchain, others) spurred on by the ongoing COVID-19 pandemic. In this age of the digital economy, financial institutions and merchants are continuously striving to improve customer experience by adding innovative services, improving omnichannel support, and facilitating frictionless purchases. However, digitization has also exposed organizations to an ever-increasing number of vulnerabilities that can be exploited for various fraudulent activities. Criminals are continuously looking at finding innovative ways to uncover these vulnerabilities and outsmart the existing fraud detection systems to launch high-volume and complex fraud attacks. In addition, regulatory environments are becoming more stringent with increasing scrutiny on cybersecurity measures as well as fraud management models. Therefore, organizations across the globe are evaluating their existing fraud detection and prevention strategies and looking at deploying advanced fraud detection technologies to actively detect and prevent frauds, minimize losses, improve fraud investigation, comply with global norms, and enhance the overall customer experience. Hence, organizations are continuously embracing sophisticated fraud solutions such as Enterprise Fraud Management (EFM) for enhanced security and to operate smoothly in these challenging environments.

An EFM solution helps organizations by providing comprehensive real-time risk monitoring and analysis of all transactions and identifying internal and external fraud covering all users, accounts, and channels. In addition, EFM solution vendors are focusing on improving their technology value proposition by enhancing the performance of their machine learning models and leveraging automation and advanced analytics to improve the accuracy and speed of fraud detection, fraud investigation, and triage. The EFM solutions' primary focus is on enhancing customer experience and providing confidence to organizations to focus on revenue optimization strategy rather than on fighting frauds. An advanced EFM platform helps implement an effective fraud management strategy and offers fundamental value propositions, including effectively detecting and preventing frauds, minimizing fraud losses, enhancing the efficiency of fraud investigations, and improving the digital experience for customers. In addition to protecting organizations from reputational and financial damage, an advanced EFM solution also aids organizations in complying with the ever-increasing global regulations. Therefore, the need for such advanced fraud prevention solutions will increase in the future.

Following are the key capabilities of enterprise fraud management (EFM) solutions:

- **Data Integration-** An EFM platform integrates the customer's historical transactional data and contextual information across all interaction channels to help improve the effectiveness of the fraud management solution, improve real-time decisioning, and reduce false positives. The platform should integrate transactional data and contextual information from across product lines, payment types, and interaction channels, including online, mobile, and in-store. The platform must also support enriching with external feeds, including public records, digital identity verification, consortiums, etc. Depending on the vendor's platform, the EFM solution can also support data ingestion from streaming data and various unstructured data sources, such as notes and call center logs, to further enhance the model’s performance.

- **Behavioral Analytics-** An EFM platform may include behavior modeling to supplement the rule engine, machine learning algorithm, AI engine, and statistical models in monitoring the user behavior across channels to detect anomalies and curb new fraud attacks. The Behavioral Analytics capability aids in continuous monitoring of user behavior and compares the same with the historical data. The capability monitors behavioral patterns like typing speed, hovering of mouse, activity time, and more robust authentication is proffered in case of any deviation from the usual activity.

- **Risk Scoring:** An EFM platform provides risk scoring of all the transactions to be used for rule or policy engines. The risk model analyzes real-time transactions and the customer's historical transactions across various segments, including client type, ownership, profession, enterprises, demographics, and others, and assigns a risk score that is prioritized based on the risk criticalities. A statistical structure is demonstrated to analyze customer risk scorings, enabling a robust compliance across multiple use cases, thereby improving the efficiency of risk investigation and customer service. For transactions or access requests with a high level of risk scores, the system demands an additional authentication step or may even block access if it deems the access request is very high risk. A low-risk score indicates trusted users, and the system lowers the authentication level to offer hassle-free access to such users. This additional level of security makes it difficult for fraudsters and bad actors to gain unauthorized access.

- **Real-time Detection and Interdiction:** An EFM platform enables the ingestion of streaming data and provides real-time decisioning to prevent fraud before it occurs. The solutions utilize advanced machine learning and artificial intelligence techniques to detect and spot the hidden anomalies in real-time and act accordingly. These sophisticated models help in saving time while offering accurate results, thereby facilitating the decision-making process.

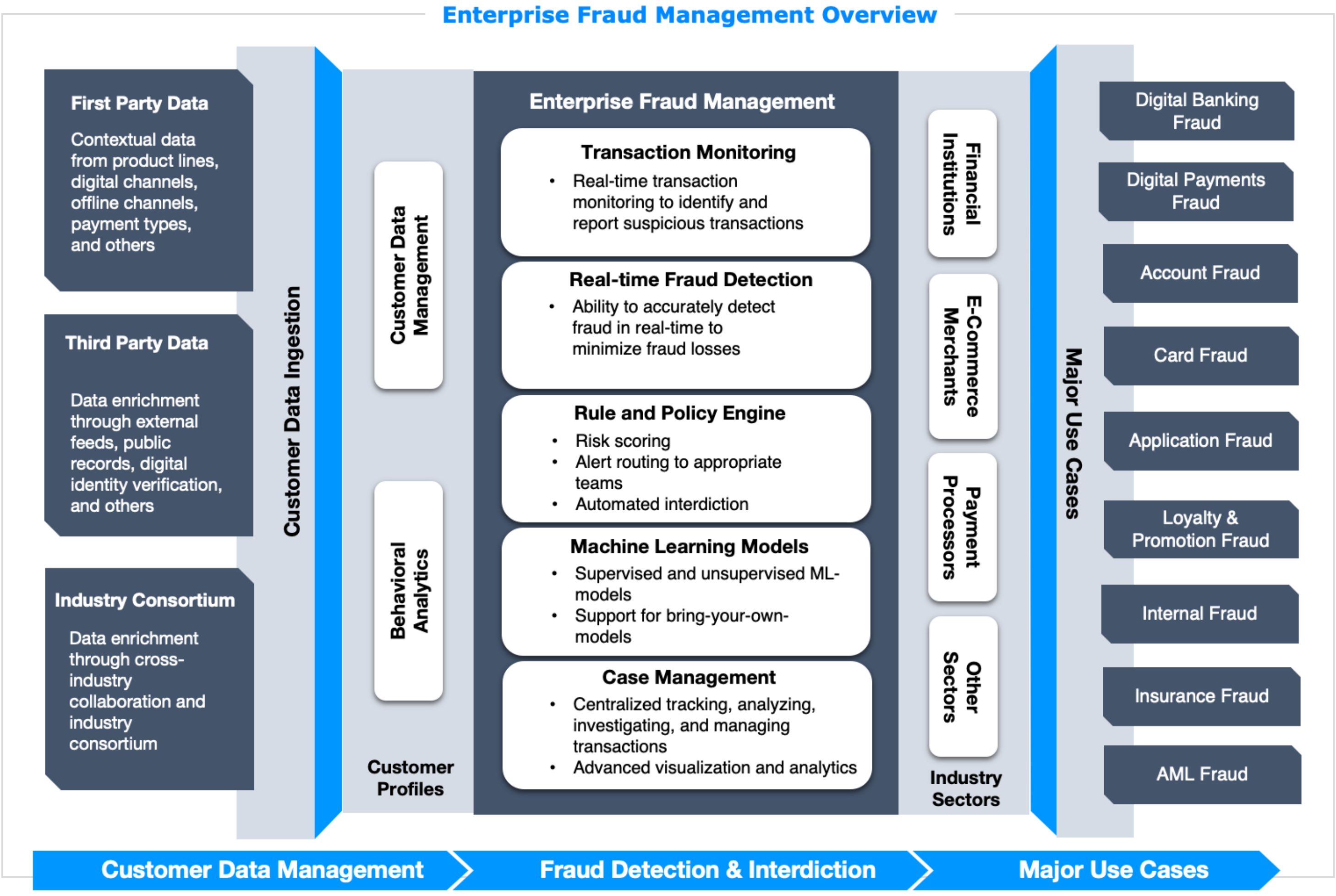
- **Alerting and Case Management:** An EFM solution offers an alert and case management capability that helps manage risk and fraud in real-time. The capability provides centralized tracking, analyzing, investigating, and managing of transactions. It provides a centralized interface with complete visibility into the critical components related to the transaction on a single screen, enabling analysts to execute appropriate actions specific to the case. Alerting helps to quickly notify and prevent high-risk login attempts. An EFM solution also provides an investigation of suspicious activities. An effective case management tool with a user-friendly interface can significantly reduce the resolution time and improve the investigation team's operational efficiency. The case management capability also helps in analyzing and marking activities as genuine or fraudulent, based on the investigation. These markings are then fed back into the risk engine to enhance the precision of the risk score of future activities.

- **Self-Service Environment:** An EFM solution provides a self-service capability that enables users to perform various actions like user ID and password recovery, password reset, etc. The capability allows users to self-register if they are new to the platform and manage their devices according to the company's policies. They can introduce a new device for authentication or remove the existing device and set up default devices. The solution also allows changes in authentication methods. For instance, users can decide if they would like to receive an OTP through email or SMS.

- **Omnichannel Support:** An EFM platform/solution provides omnichannel support. The functionality allows different types of external systems to connect to the same platform. It touches all the external and internal touchpoints of fraud during the entire customer journey. The capability considers a customer-centric approach rather than a fraud-centric or channel-centric approach. It consolidates all activities for each account holder in any channel to create a unified view of that respective customer's behavior and then analyzes the blended data to look for suspicious or high-risk activity in the context of the account holder's recent and historical actions.

- **Visualization and Reporting:** An EFM solution offers centralized visualization capabilities. These capabilities include a unified view of the network data, user behavior patterns, system data, and application data to help organizations navigate large datasets. The capability gathers and collates data from numerous sources, and the compiled data is presented in a single graphical presentation to make it easier to understand and analyze. EFM solutions use numerous data visualization techniques, including link analysis, graph analysis, etc., to scrutinize huge datasets and detect any peculiar activity. Reporting is a significant capability in an EFM solution. It generally refers to generating reports to get a unified view pertaining to the risk profiles, fraud patterns, active anomalies, devices with potential malware, ongoing trends, etc. These reports are submitted for internal audits to the higher authorities, commonly known as internal reporting, and are also used for complying with external reguations.

Figure: Key Components of Enterprise Fraud Management (EFM) Solution.



Enterprise Fraud Management Overview

First Party Data

Contextual data from product lines, digital channels, offline channels, payment types, and others

Third Party Data

Data enrichment through external feeds, public records, digital identity verification, and others

Industry Consortium

Data enrichment through cross-industry collaboration and industry consortium

Customer Data Ingestion

Customer Data Management

Behavioral Analytics

Customer Profiles

Enterprise Fraud Management

Transaction Monitoring

- Real-time transaction monitoring to identify and report suspicious transactions

Real-time Fraud Detection

- Ability to accurately detect fraud in real-time to minimize fraud losses

Rule and Policy Engine

- Risk scoring
- Alert routing to appropriate teams
- Automated interdiction

Machine Learning Models

- Supervised and unsupervised ML-models
- Support for bring-your-own-models

Case Management

- Centralized tracking, analyzing, investigating, and managing transactions
- Advanced visualization and analytics

Financial Institutions

E-Commerce Merchants

Payment Processors

Other Sectors

Industry Sectors

Major Use Cases

Digital Banking Fraud

Digital Payments Fraud

Account Fraud

Card Fraud

Application Fraud

Loyalty & Promotion Fraud

Internal Fraud

Insurance Fraud

AML Fraud

Customer Data Management → Fraud Detection & Interdiction → Major Use Cases

Source: Quadrant Knowledge Solutions

Factors Influencing Market Development and Growth

The following dominant technology and market developments are influencing the growth of the overall global enterprise fraud management market:

Growing Frequency, Sophistication, and Complexity of Fraud and Cybersecurity Attacks are Significantly Expanding the Organization's Risk Exposure

The fraud and cybersecurity attacks are growing in number, sophistication, and complexities while continuously expanding the risk exposure to financial institutions and e-commerce organizations. In recent years, global organizations have observed an increasing number of fraud attacks, including application fraud, account takeover, card-not-present fraud, bot attacks, cybersecurity breaches, and internal fraud. The growing complexity of fraud attacks drives the need for advanced fraud detection and management technologies to prevent significant financial and reputational loss. Additionally, cybercriminals are increasingly targeting mobile channels for login attacks as customers across the globe are increasingly adopting mobile applications for various financial transactions and online sessions.

With the advancements of technology, attackers are using sophisticated techniques like advanced artificial intelligence, automation, and machine learning to launch complex attacks. Traditional rule-based fraud prevention systems are not effective in detecting new types of fraud and suspicious activities.

The effectiveness of the traditional fraud prevention systems has been challenged by an unprecedented rise in cyberattacks fuelled by the digitalization of businesses and the COVID-19 pandemic. The pandemic has forced employees to work remotely, increasing online activities and adopting BYOD/ WYOD policies. The growing number and sophistication of fraud attacks require a flexible, scalable, and advanced enterprise fraud management solution to address continuously changing fraud and cyber-attack dynamics. Therefore, organizations are increasingly evaluating vendors with robust ML-based fraud detection solutions, emphasizing model performance.

Emerging Business Models are Leading the Wave of Emerging Fraud Trends

The rapid adoption of innovative consumer technologies is transforming banking, financial services, retail, and other industries. Customers expect organizations to have a presence across digital, mobile, and emerging channels to provide a consistent and personalized experience. Driven by the continued advancements, organizations and consumers are increasingly embracing emerging technologies to perform various operations. Businesses are steadily providing services through emerging models, including social banking through social media platforms, voice banking enabled by voice-controlled virtual assistants like Alexa, chatbots, and IoT payments.

While emerging business models drive customer-centric strategies across organizations, cybercriminals are getting new avenues for conducting fraudulent activities like bot attacks, synthetic identities, and fraud network attacks. Organizations must conduct a thorough analysis of the impact of emerging channels and added vulnerabilities and adopt strategies based on the emerging financial crime landscape. Leading EFM vendors are continuously updating their functionalities to support the organization's emerging business models. Additionally, the vendors are increasingly educating and demonstrating the value proposition of advanced fraud detection solutions over traditional systems to prevent emerging fraud trends.

Growing Adoption of Digital Banking Strategies

Digitalization across different industry verticals has significantly raised customer expectations from banks to offer a secure and consistent experience across all digital channels. While banking organizations continue to support digital channels as a primary way for customer engagement for various services, a hassle-free customer experience is becoming the primary competitive differentiation for the global banking industry.

Digital strategies have significantly improved banking operations and customer service across a range of banking products. However, it has also resulted in increased vulnerabilities of fraud and cybersecurity risks. Globally, digital banking fraud cases are growing exponentially. The risk landscape is expanding significantly due to several factors such as increased usage of mobile apps by consumers for various financial transactions, complex technology landscape, and the rapid growth of IoT devices. Additionally, banking organizations are increasingly concerned about the growing complexities around confidential data and information security due to real-time payments and open banking. As open banking allows third-party to gain access to customer’s confidential data through APIs, there is a high probability of customer data breaches. Therefore, banking organizations are increasingly replacing their legacy systems with advanced fraud management systems, which aid in minimizing false-positive rates and flagging fraudulent activities. The banking organizations are looking at fraud management systems powered by advanced self-learning and machine learning models that detect known, unknown, and emerging fraud types.

EFM Vendors are Increasingly Leveraging Industry Consortium and Shared Intelligence

Industry consortium network enables trusted cross-industry peers to share data about shared risks for various use cases. Organizations will gain access to an accurate view of users' identities and risk landscape by leveraging real-time data from industry peers. In addition to internal and external data sources, the rich shared intelligence from consortiums can augment the effectiveness of fraud models in fighting the most advanced and emerging frauds.

Leading EFM vendors are increasingly incorporating consortium-based shared intelligence from the entire payment ecosystem to integrate rich datasets into their machine learning models. It helps data scientists train their ML models and make regular updates to detect emerging unknown fraud patterns. The emerging vendors with no access to shared intelligence or industry consortium data focus on providing advanced unsupervised machine learning models to detect emerging fraud patterns. Leveraging industry consortium and shared intelligence enabled organizations to provide shared features for creating custom models to meet unique business needs.

Growing Adoption of Cloud-based Deployments

The majority of large enterprises from various industries are moving towards a cloud-first strategy to deploy enterprise software and business systems. However, cloud-based solutions are still in the emerging stage since most large banking organizations still prefer on-premises deployment. Growing complexities of global and regional regulations, data security, and privacy issues continue to impact the adoption of cloud-first strategies by large banking organizations. However, driven by the advancements in security technologies and the growing confidence of cloud platforms, the scenario is gradually shifting. Global Banking and financial service organizations are increasingly gaining confidence in cloud security and are moving towards cloud-based deployments.

Cloud-based deployment offers a significant advantage in terms of scalability, flexibility, automatic upgradations, and cost-effectiveness. Additionally, vendors ensure that organizations always have access to the latest version of the solution with regular updates, maintenance, and support services. Further, small and mid-sized businesses often lack resources in deploying cutting-edge technologies and are associated with the same sets of operational challenges as large organizations. Thereby, SMB organizations usually prefer cloud-based deployments to cut operational costs and gratify their needs with a low monthly/yearly charge.

Rise in Adoption of AI, ML, Automation, and Advanced Analytics to offer Advanced EFM Capabilities

Financial Services firms are cognizant of the importance of key technologies such as AI, ML, and automation play in improving the efficiencies in detecting and mitigating risks significantly. An AI-driven fraud management platform can integrate data from multiple sources to drive actionable intelligence in detecting, analyzing, investigating, and resolving a large volume of alerts and cases. Therefore, many leading enterprise fraud management vendors are constantly leveraging automation, machine learning, and AI in automating repetitive tasks and manual processes to improve process efficiency, resource utilization, and productivity. It also assists the analysts in selecting appropriate models to be used specifically to various fraud and anti-money laundering (AML) use cases. The growing complexities in data patterns and increasing focus on strengthening the fraud prevention strategies will drive EFM vendors to increasingly leverage automation, machine learning, and AI in automating repetitive tasks and manual processes to help enterprises improve process efficiency, resource utilization, and productivity, protect customers and improve overall customer experience.

With the increasing amount of financial data, usage of digital payments, false positives, and data complexity, there is a growing need for end-to-end fraud management solutions that can intelligently address the challenges across the constantly changing threat landscape with greater speed and accuracy. Therefore, leading vendors are focusing on adopting the combination of supervised and unsupervised models to help enterprises gain better insights into the customer accounts, speed up the fraud prevention processes, facilitates real-time scoring, and reduce false positives. Owing to growing emphasis for minimizing human intervention and apply policies, rules, operational workflows and frameworks to eliminate errors, improve response rates and increase the process speed, vendors are increasingly adopting RPA capabilities to help enterprises reduce fraud losses. EFM vendors also enable enterprises to combine RPA with third-party intelligence to protect customers from online and mobile banking fraud. In addition, advanced fraud prevention solutions offer omnichannel fraud management capabilities and provide the ability to accurately capture and comprehend complex relevant data types and help enterprises adopt a proactive approach to fraud management. Leading EFM vendors are also increasingly integrating behavioral biometrics technology to improve the accuracy of fraud prevention. Backed by AI, behavioral biometrics recognize the user’s gestures such as typing speed of the keyboard, hovering of the mouse, taps and touch on a mobile screen, etc. and compares these gestures with the known digital behavioral traits that are common to fraudsters, bots, and trusted users. Behavioral biometrics is used to detect bots, recognize good customer profiles, and identify unusual interactions.

Competitive Landscape and Analysis

Quadrant Knowledge Solutions conducted an in-depth analysis of major enterprise fraud management (EFM) vendors by evaluating their products, market presence, and value proposition. The evaluation is based on primary research with expert interviews, analysis of use cases, and Quadrant's internal analysis of the overall EFM market. This study includes an analysis of key vendors, including ACI Worldwide, BAE Systems, BPC, Clari5, DataVisor, EastNets, Featurespace, Feedzai, FICO, Fiserv, IBM, LexisNexis Risk Solutions, NICE Actimize, Quantexa, and SAS.

NICE Actimize, IBM, SAS, Feedzai, ACI Worldwide, Featurespace, BPC, Eastnets and DataVisor are the top performers and technology leaders in the global EFM market. They deliver comprehensive EFM solutions to address a variety of EFM use cases.

NICE Actimize has received the highest ratings across the performance parameters of technology excellence and customer impact. The company's integrated fraud management platform named IFM-X offers real-time and end-to-end fraud prevention coverage. NICE Actimize's IFM-X platform is backed by AI and advanced analytics, facilitating high accuracy in detection and decisioning, and enrichment during triage and investigations. IFM-X platform is also powered by machine learning (ML) analytics which continuously learns, discovers, and adapts to offer the necessary agility to detect anomalies and proactively prevent fraud.

IBM has also received the high ratings for its EFM platform, Trusteer, which collects and evaluates numerous digital signals, including device, session data, user activity, behavioral biometrics, malware, spoofing evidence, fraud consortium, BOT indication, abnormal session activity, and transactional data. It determines risk and detects active fraud attacks irrespective of device types such as mobile and desktop. IBM's human analytics services are combined with ML models, which include darknet and threat research. The company has an intelligence network that analyzes digital identity attributes, thereby facilitating evidence for fraud.

SAS is amongst the largest vendors in the advanced analytics, business intelligence, and fraud management market. The company offers advanced analytics capability and a unique 'signatures' approach to support multiple entities. Additionally, it provides advanced neural network modeling for faster fraud detection and better hybrid modeling. It integrates pooled consortium data into bank-specific models while offering champion/challenger functionality and the ability to deploy and monitor multiple fraud models. With the company's zero-footprint technology, the solution can be deployed across various sites with minimal cost.

Feedzai's innovative technology value proposition is driven by advanced, real-time machine learning capabilities to detect and thwart known and unknown fraud attacks.

The company offers solutions in an omnichannel environment with responsible AI, Segment-of-One Profiles™, and Feedzai's Genome. It also includes white-box explanations for targeted investigation across the depth and breadth of the cloud experience.

ACI Worldwide offers a robust integration between its proactive risk manager (PRM) and payment solutions. It leverages fraud intelligence from its vast payment ecosystems to provide an effective fraud detection solution. The company offers ACI network intelligence, an operational control center, and an ACI case manager. ACI helps orchestrate cross-industry collaboration across business partners, third parties, and the ACI community, adding significant value to PRM. ACI Model Generator (AMG) further adds value to PRM by enabling business users to create, test, and deploy their custom machine learning models. Network intelligence enables organizations to leverage shared features for creating custom, hybrid, and consortium-based models to meet unique business needs.

Featurespace offers a robust technology value proposition with its adaptive behavioral biometrics and real-time machine learning models. The company has demonstrated real-time fraud detection, robust model performance, transparency, and configurability to offer customizable solutions for multiple use cases. The ARIC risk Hub platform's rules in propriety AMDL language and enables users to build and maintain rules without coding knowledge. The platform supports a multi-tenancy architecture and an open modeling environment allowing users to write and test models in ARIC.

BPC offers comprehensive fraud detection capabilities and omnichannel case management for banking and financial service organizations. The company provides robust experience, domain knowledge, and service capabilities for payment solutions and fraud management solutions in the financial service industry. BPC's SmartVista fraud management solution includes omnichannel fraud prevention, self-serviceable machine learning models, and a low-code platform.

Eastnets's PaymentGuard solution is powered by technologies such as AI-backed machine learning detection models that allow organizations and FIs to stay alert against upcoming fraud threats. PaymentGuard solution includes a standard model library that contains models to cover a wide range of fraud patterns across all channels offering cross-channel and multi-channel, fast implementation cycle, and advanced SWIFT payment fraud solutions in the market. It also provides advanced analytics and link analysis capability to gain a unified view of a customer's current and past activities through unified dashboard.

DataVisor is an emerging leader with innovative technology value proposition. The company's dCube platform offers a powerful detection engine based on the combination of unsupervised ML models, supervised ML models, and deep learning to provide layered protection against sophisticated frauds.

FICO, BAE Systems, Fiserv, LexisNexis Risk Solutions, Clari5, and Quantexa are positioned as challengers. **FICO** is placed as a major challenger in Quadrant's EFM SPARK Matrix, 2021. It offers strong domain expertise in the payment industry, and the company provides a scalable platform and superior model performance in the global EFM market. FICO provides comprehensive fraud analytics capabilities backed by real-time behavioral profiling, supervised and unsupervised machine learning models, and adaptive analytics.

BAE Systems offers robust case management and workflow and libraries of pre-packaged fraud rules capabilities for its EFM solution. The company coupled predictive analytics with machine learning techniques for spotting suspicious behavior. **Fiserv** placed as a challenger in Quadrant's EFM SPARK Matrix, 2021 offers advanced capabilities for card fraud and offers libraries of pre-packaged fraud rules. **LexisNexis Risk Solutions** uses strong consortium-based intelligence feed for its models to enhance the effectiveness of its EFM performance. LexisNexis Risk Solutions applies a combination of physical and digital identities such as device, behavioral biometric, and credit-seeking insights, providing a holistic view to the customers.

Clari5 placed as an emerging challenger offers a real-time intelligent big data solution that monitors suspicious activities and combats fraud in real-time. Clari5's EFM solution meets the fraud detection, investigation, prevention, monitoring and compliance. **Quantexa** another emerging challenger offers advanced analytics, detection of anomalies at scale, and greater context to decision-makers. The company also offers advanced and proprietary fraud-detection techniques.

Key Competitive Factors and Technology Differentiators

A majority of the leading EFM vendors may provide capabilities including data integration, behavioural analytics, a robust risk scoring engine, real-time detection and interdiction, alerting and case management, self-service environment, omni-channel functionality and visualization and reporting. However, the breadth and depth of functionalities may differ by different vendors offerings. Driven by increasing competition, vendors are increasingly looking at improving their technology capabilities and overall value proposition to remain competitive. Some of the key competitive factors and differentiators for the evaluation of EFM vendors are as follows.

- **Sophistication of Technology Capabilities:** Users should evaluate an EFM solution that offers comprehensive capabilities, including data ingestion from internal and external sources, user and entity behavior analytics, automated risk scoring, real-time fraud detection and interdiction, integrated case management, advanced modeling and rule-engine, cloud-based deployment offering, scalability and uptime, and open technology architecture. Additionally, the vendor's customer value proposition may differ in terms of ease of deployment, ease of use, price/performance ratio, support for a broad range of fraud and AML use cases, and global support service.

- **Comprehensive Data Integration Capability:** Vendors' capability to provide comprehensive data integration is essential in improving the performance of the fraud detection models. A few vendors may support data ingestion just from out-of-the-box transactional data, account information, and basic customer profiles. In such instances, organizations are required to invest significant efforts in acquiring data from additional sources. An EFM platform should support comprehensive capability to integrate a large volume of data in multiple formats and from contextual data sources across all payment types, channels, and product types. Leading vendors are also providing behavior biometrics and analytics capability to monitor and continuously authenticate user (and entity) behavior across channels to identify known attacks and unknown indicators of compromise. Few vendors may also support the shared intelligence approach with data ingestion from an industry consortium. Users should evaluate vendors that offer holistic cross-channel fraud prevention capabilities. The EFM platform should accept data from various channels, product types, and payment methods. In addition, the platform should provide a holistic view of each account holder across any channel in real-time by providing insights on customer behavior and new activities across channels, historical and current patterns that help to analyze suspicious transactions

- **Effectiveness of Case Management:** An effective case management functionality is essential in visualizing the perspectives of the customer activities holistically across the omnichannel environment to enable the analyst and investigators to determine whether the financial activity is legitimate or fraudulent. Organizations' limited investigation resources are proving to be hurdles ensuring timely handling of an ever-increasing number of fraud cases. An effective case management tool helps improve the investigation team's operational efficiency and ensures maximum resource utilization for a faster case resolution. While a majority of the EFM vendor provides case management functionalities, the effectiveness in augmenting the operational efficiencies of the investigation team working on multiple complicated and lengthy financial crime cases is essential. Therefore, leading EFM vendors are providing advanced case management with process automation capability that helps automate repetitive and manual operations of the investigation processes. The case with high priority is placed at the top of the queue and is reviewed on priority by the analyst and investigators. Apart from these capabilities, the case management functionality should also offer an intuitive dashboard, alert management, management reporting, fraud loss analysis, and regulatory compliance features.

- **Open Framework and Bring Your Own Model (BYOM) Support:** Typically, global financial institutions and large merchants have internal data science teams and often prefer to utilize their in-house developed machine learning models. However, a few vendors may force the organizations' internal data scientist team to work with the vendor's proprietary machine learning models, language, tools, and libraries. Additionally, organizations may be required to use vendors' professional services to implement and customize models to suit specific use cases. Organizations often incur additional costs and delay in overall implementation. Enterprise fraud management platforms should support an open system framework and facilitate easy imports of third-party models built using any language, platform, and library. The platform may also support Predictive Model Mark-up Language (PMML) for easy imports without custom coding. Leading EFM vendors also support custom model development,

- **Model Performance:** Model performance is a key differentiator as the presently available multiple fraud management solutions in the market can have significantly differing performances. The traditional rule-based fraud detection system is no longer effective in responding quickly to new attack vectors or fraud patterns and preventing frauds. Additionally, the traditional machine learning models, which are mostly refreshed every year, are not sufficient to fight fraudsters using increasingly sophisticated techniques. Also, continuous monitoring and updating of machine learning models are essential to adapt to emerging fraud patterns and evolving threat landscape. Therefore, organizations should evaluate model performance in terms of speed and accuracy of fraud detection with low false positives.

- **Scalability and Availability:** Global financial institutions and large eCommerce merchants often require a fraud management solution that can provide the requisite speed, scalability, latency, and availability to meet their distributed payment environment across the lines of businesses, payment types, channels, and geographical locations. The platform should support scalability to process a large volume of transactions per second (TPS) with sub-second response times. Organizations should evaluate vendors platforms' capability to support a large volume of real-time transactions with sub-second response time. Users should evaluate vendors that support scalable data processing capabilities powered by AI/ML and automation capabilities.

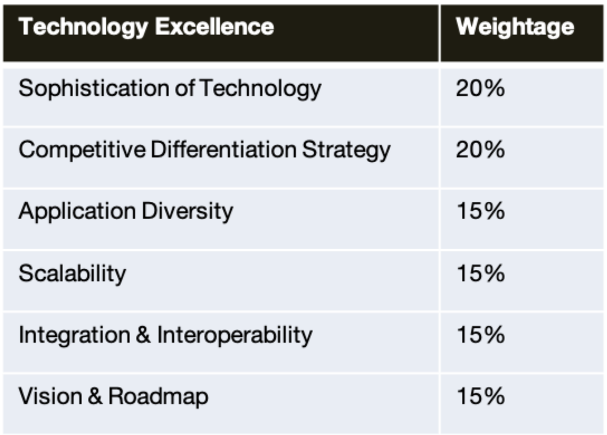
- **Technology Vision:** The threat landscape is consistently evolving to include automated rapid attacks, botnet attacks, sophisticated targeted attacks, and other such attacks targeting organizations for various fraudulent and criminal activities. Users should carefully select the right technology partner per their digital transformation roadmap, specific use case, and emerging fraud trends. EFM vendors are consistently improving their technology value proposition in terms of providing comprehensive coverage for traditional and emerging payment types in the omnichannel environment. Leading EFM vendors are also providing advanced functionalities to support automated threat detection, investigation, and response, easy data integration, custom model development, automated feature engineering, and advanced fraud intelligence from the consortium and multiple third-party sources to augment the performance of their enterprise fraud management solutions.

- **Vendor's Expertise and Domain Knowledge:** Organizations should evaluate the vendor's expertise and domain knowledge in understanding their unique business problems, use case, and industry-specific requirements. Organizations are advised to conduct a comprehensive evaluation of different EFM platforms and vendors before making a purchasing decision. Users should employ a weighted analysis of several factors important to their specific organization's use cases and industry-specific requirements. Requirements of key EFM features may differ significantly from financial institutions to eCommerce merchants, from SMB to large enterprise organizations, and such others. Users should also look for an EFM solution with a history of successful large-scale deployments and carefully analyze the existing case studies of those deployments. This should form the basis to prepare the best practice for enterprise fraud management platform deployments.

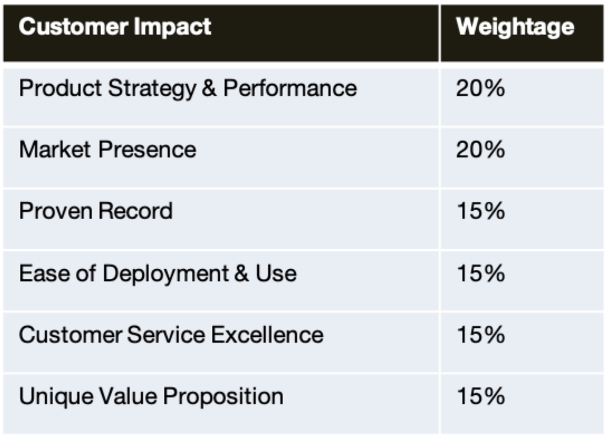
SPARK Matrix™: Strategic Performance Assessment and Ranking

Quadrant Knowledge Solutions' SPARK Matrix provides a snapshot of the market positioning of the key market participants. SPARK Matrix provides a visual representation of market participants and provides strategic insights on how each supplier ranks related to their competitors, concerning various performance parameters based on the category of technology excellence and customer impact. Quadrant's Competitive Landscape Analysis is a useful planning guide for strategic decision makings, such as finding M&A prospects, partnership, geographical expansion, portfolio expansion, and others.

Each market participant is analyzed against several parameters of Technology Excellence and Customer Impact. In each of the parameters (see charts), an index is assigned to each supplier from 1 (lowest) to 10 (highest). These ratings are designated to each market participant based on the research findings. Based on the individual participant ratings, X and Y coordinate values are calculated. These coordinates are finally used to make SPARK Matrix.



Technology Excellence	Weightage
Sophistication of Technology	20%
Competitive Differentiation Strategy	20%
Application Diversity	15%
Scalability	15%
Integration & Interoperability	15%
Vision & Roadmap	15%



Customer Impact	Weightage
Product Strategy & Performance	20%
Market Presence	20%
Proven Record	15%
Ease of Deployment & Use	15%
Customer Service Excellence	15%
Unique Value Proposition	15%

Evaluation Criteria: Technology Excellence

- **The sophistication of Technology**: The ability to provide comprehensive functional capabilities and product features, technology innovations, product/platform architecture, and such others
- **Competitive Differentiation Strategy**: The ability to differentiate from competitors through functional capabilities and/or innovations and/or GTM strategy, customer value proposition, and such others.
- **Application Diversity**: The ability to demonstrate product deployment for a range of industry verticals and/or multiple use cases.

- **Scalability**: The ability to demonstrate that the solution supports enterprise-grade scalability along with customer case examples.
- **Integration & Interoperability**: The ability to offer product and technology platforms supporting integration with multiple best-of-breed technologies, providing out-of-the-box integrations, and open API support and services.
- **Vision & Roadmap**: Evaluation of the vendor's product strategy and roadmap with the analysis of key planned enhancements to offer superior products/technology and improve the customer ownership experience.

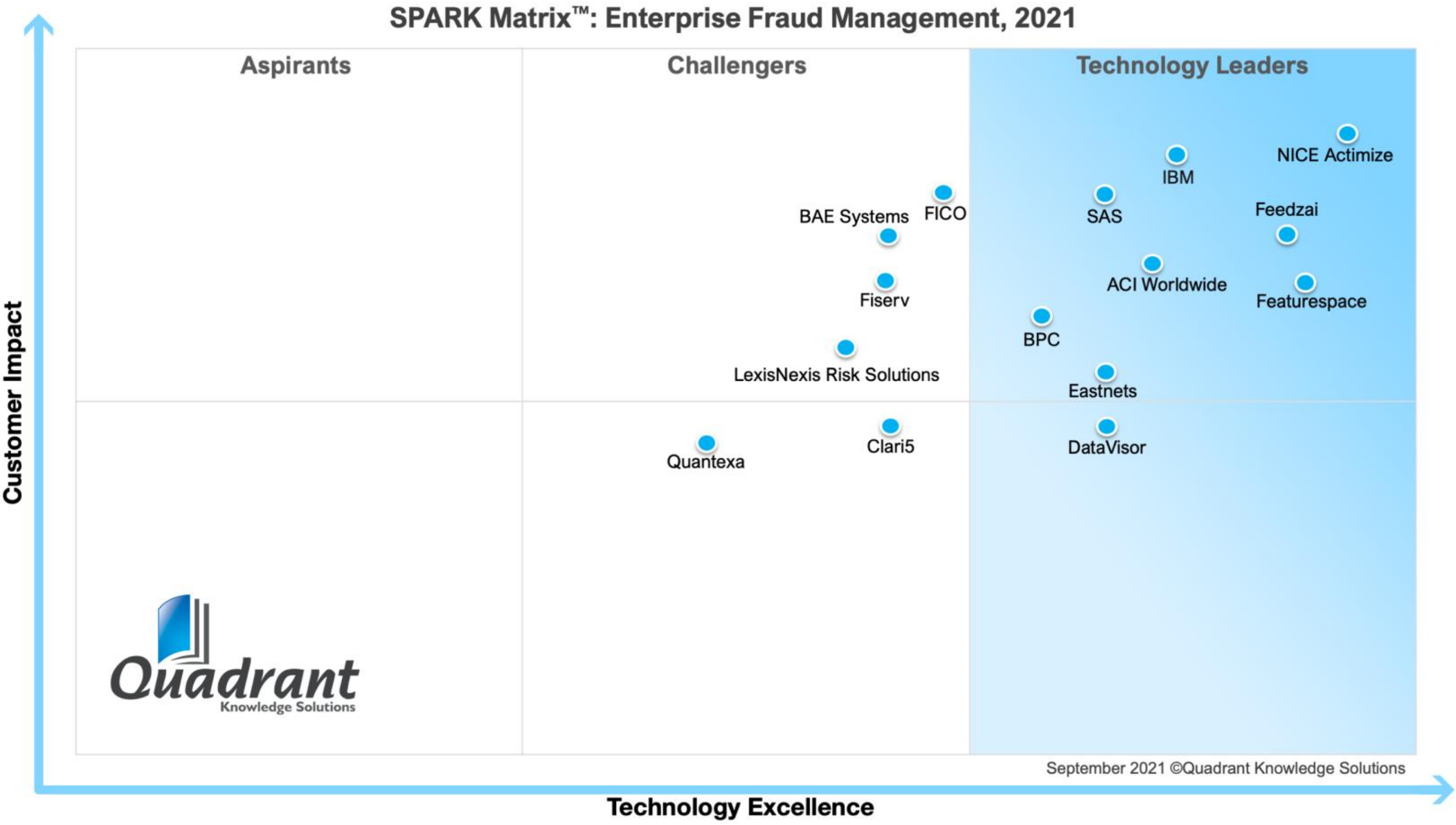
Evaluation Criteria: Customer Impact

- **Product Strategy & Performance**: Evaluation of multiple aspects of product strategy and performance in terms of product availability, price to performance ratio, excellence in GTM strategy, and other product-specific parameters.
- **Market Presence**: The ability to demonstrate revenue, client base, and market growth along with a presence in various geographical regions and industry verticals.
- **Proven Record**: Evaluation of the existing client base from SMB, mid-market and large enterprise segment, growth rate, and analysis of the customer case studies.
- **Ease of Deployment & Use**: The ability to provide superior deployment experience to clients supporting flexible deployment or demonstrate superior purchase, implementation, and usage experience. Additionally, vendors' products are analyzed to offer a user-friendly UI and ownership experience.
- **Customer Service Excellence**: The ability to demonstrate vendors capability to provide a range of professional services from consulting, training, and support. Additionally, the company's service partner strategy or system integration capability across geographical regions is also considered.
- **Unique Value Proposition**: The ability to demonstrate unique differentiators driven by ongoing industry trends, industry convergence, technology innovation, and such others.

SPARK Matrix™: Enterprise Fraud Management (EFM)

Strategic Performance Assessment and Ranking

Figure: 2021 SPARK Matrix™
(Strategic Performance Assessment and Ranking)
Enterprise Fraud Management Market



Vendor Profiles

Following are the profiles of the leading EFM vendors with a global impact. The following vendor profiles are written based on the information provided by the vendor's executives as part of the research process, along with publicly available information. The Quadrant research team has also referred to the company's website, whitepapers, blogs, and other sources for writing the profile. A detailed vendor profile and analysis of all the vendors, along with various competitive scenarios, are available as a custom research deliverable to our clients. Users are advised to directly speak to respective vendors for a more comprehensive understanding of their technical capabilities. Users are advised to consult Quadrant Knowledge Solutions before making any purchase decisions regarding EFM technology and vendor selection based on research findings included in this research service.

ACI Worldwide

URL: https://www.aciworldwide.com/

Founded in 1975 and headquartered in Miami, Florida, USA, ACI Worldwide is a provider of real-time digital payments software and solutions. ACI offers Proactive Risk Manager (PRM), a flagship product for Enterprise Risk, which is a part of its ACI Fraud Management (PRM) solution. Proactive Risk Manager is specifically designed for financial institutions to combat fraud and money laundering schemes by coordinating sources and integrating risk services. The PRM solution offers key capabilities and features, including integration & orchestration, machine learning, network intelligence, analytics engine, alerting and case management.

The PRM integration and orchestration engine offers the ability to integrate and orchestrate multiple data sources in a single solution and combines external data through open APIs or web services to perform data enrichment. It uses configurable workflow capabilities, content management, and validation to transform the data received. PRM performs all fraud and AML checks across channels, geographies, and lines of business in real or near-real-time to detect potential risk. It identifies risks at authorization to protect real-time payment transactions.

Powered by a machine learning capability, ACI's Adaptative Model Generator is designed for rapid deployment and ease of use. It adaptively meets the requirements of any modern fraud operations capability, as it creates customized machine learning models in hours to launch fraud prevention strategies.

ACI Worldwide uniquely offers a Network intelligence capability, a proprietary technology to enhance fraud prevention strategies. The capability enables banks, processors, acquirers, and networks to securely share and consume industry-wide fraud signals to feed their machine learning models alongside proprietary data. The capability also allows users to share intelligence across various networks and jurisdictions, thus eliminating the need to share the private or personal data of clients. The solution offers shared features for consortium-based models, hybrid models based on private & public features, and central infrastructure oversight of fraud trends.

ACI Worldwide's analytics engine aids in the filtration of rules created to focus specifically on identified conditions that match the business needs of the fraud prevention strategy. These rules are deployable in real-time (in the authorization path) or near real-time (post-authorization), and the tester function allows proposed rules to be assessed for impact before deployment. The advanced rules analytics engine consistently upgrades the fraud trends, and the sophisticated rules strategy simulation feature enables the user to retrospectively scrutinize the rules, ensuring the ruleset is fully optimized and delivering the best false-positive and detection rates.

The PRM solution provides end-to-end alerting and case management capability for fraud investigations and resolutions. The capability notifies customers, branches, and merchants with alerts about likely fraud with push and pull notification features through SMSes. ACI Case Manager delivers key features, including business intelligence to offer fraud trends and areas of risk, reporting, attachment manager, workflow, and role-based access control security. The product provides a framework that defines processes for researching and resolving cases, including investigation resources, time frames, escalation paths, and alerts. ACI's alerting and case management capability enables alert prioritization and creates and maintains customized behavioral profiles for anomaly detection.

ACI's risk management solution includes a Proactive Risk Management Scoring Engine (PSE), a Universal Scoring Engine (USE), and a third-party scoring engine with third-party models. PSE is ACI's proprietary engine that guarantees payments-grade non-functional requirements (NFRs) and empowers ACI neural models built by ACI data scientists. ACI's neural models are based on historical data and confirmed fraud. These models leverage the existing library of features and custom-built features to cover the organization's specific channels, products, services, and risks. The PRM Scoring Engine generates risk scores and provides logic for scores which can be used for decision making to enhance detection capabilities. USE is ACI's proprietary engine that enables third-party or custom-build PMML (predictive machine markup language) models to be integrated as per the organization's unique needs. With ACI risk orchestration, PRM can also receive and use scores generated by third-party engines and models.

The company supports both on-premises and cloud deployment models, including private and public cloud, and offering its Fraud Management Subscription service in Microsoft Azure.

Analyst Perspective

Following is the analysis of ACI Worldwide's capabilities in the global enterprise fraud management (EFM) market:

- ACI Worldwide offers ACI Fraud Management, an EFM solution to manage risk and fraud for the banking and finance vertical. The solution's real-time payment fraud prevention feature is backed by machine learning and rules technologies and aids in the prevention of fraud and other financial crimes. Furthermore, it performs real-time fraud payment screening. With customer authentication features, the solution delivers complete Strong Customer Authentication (SCA) compliance with value-added capabilities, thereby enabling an SCA exemptions strategy.

- Some of the key differentiators for ACI Worldwide include ACI network intelligence, operational control center, and ACI case manager. ACI, orchestrated with cross-industry collaboration across business partners, third parties, and the ACI community, adds significant value to PRM. ACI Model Generator (AMG) further adds value to PRM by enabling business users to create, test, and deploy their custom machine learning models. Network intelligence enables organizations to leverage shared features for creating custom, hybrid, and consortium-based models to meet unique business needs.

- ACI's operational control center offers a comprehensive set of tools to support fraud prevention operations. The center comprises perspective management with a 360-degree view of risk scenarios, intelligent alert distribution, dashboarding and reporting, and ability to perform manual and automated actions, and case & dispute management. ACI Case Manager, is integrated with PRM solutions and aids organizations in managing enterprise-wide cases efficiently.

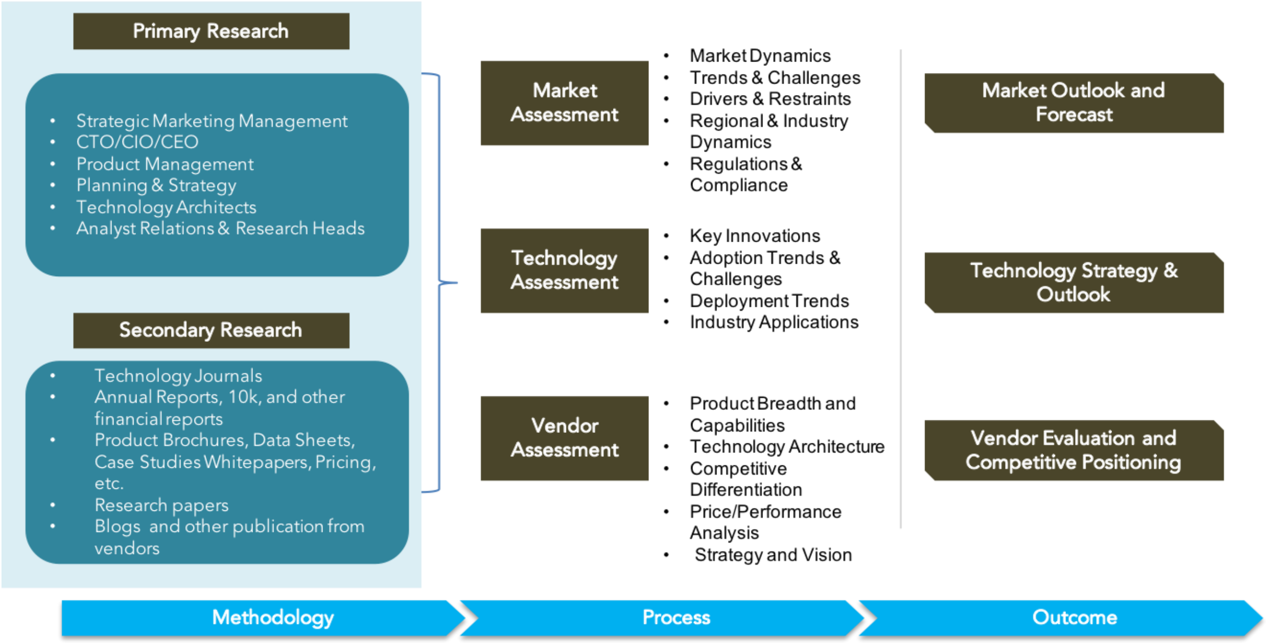
- In terms of geographical presence, ACI Worldwide has a strong presence in the US and Canada, followed by Latin America and EMEA. Concerning industry vertical perspective, the company caters to banks (retail and wholesale/transaction) as well payment processors, acquirers, PSPs, central infrastructures and card networks.

- ACI Worldwide's primary challenges include the growing competition from emerging vendors with competitive solutions offerings. However, with its industry-leading payment intelligence, strong domain experience, and professional service capabilities, ACI is well-positioned to offer strong technology and customer value propositions to meet the needs of SMB, mid-market, and large organizations.

- Concerning roadmap, ACI Worldwide is focused on adding new capabilities within the ACI Model Generator platform, including the option to run AMG as a standalone application and support for new machine learning reporting and data visualizations. The company has plans to enhance PRM with advanced AI and machine learning models and offer full cloud-native support and porting. For AML enhancements, ACI is focused on including additional investigation management and data enrichment features and UI Optimization for workflow management. For business intelligence, the company is focused on developing new reporting capabilities using advanced technologies and third-party reporting tools.

Research Methodologies

Quadrant Knowledge Solutions uses a comprehensive approach to conduct global market outlook research for various technologies. Quadrant's research approach provides our analysts with the most effective framework to identify market and technology trends and helps in formulating meaningful growth strategies for our clients. All the sections of our research report are prepared with a considerable amount of time and thought process before moving on to the next step. Following is a brief description of the major sections of our research methodologies.


Primary Research
Strategic Marketing Management
CTO/CIO/CEO
Product Management
Planning & Strategy
Technology Architects
Analyst Relations & Research Heads
Secondary Research
Technology Journals
Annual Reports, 10k, and other financial reports
Product Brochures, Data Sheets, Case Studies Whitepapers, Pricing, etc.
Research papers
Blogs and other publication from vendors
Market Assessment
Market Dynamics
Trends & Challenges
Drivers & Restraints
Regional & Industry Dynamics
Regulations & Compliance
Technology Assessment
Key Innovations
Adoption Trends & Challenges
Deployment Trends
Industry Applications
Vendor Assessment
Product Breadth and Capabilities
Technology Architecture
Competitive Differentiation
Price/Performance Analysis
Strategy and Vision
Market Outlook and Forecast
Technology Strategy & Outlook
Vendor Evaluation and Competitive Positioning
Methodology
Process
Outcome

Secondary Research

Following are the major sources of information for conducting secondary research:

Quadrant's Internal Database

Quadrant Knowledge Solutions maintains a proprietary database in several technology marketplaces. This database provides our analyst with an adequate foundation to kick-start the research project. This database includes information from the following sources:

- Annual reports and other financial reports
- Industry participant lists
- Published secondary data on companies and their products
- Database of market sizes and forecast data for different market segments
- Major market and technology trends

Literature Research

Quadrant Knowledge Solutions leverages on several magazine subscriptions and other publications that cover a wide range of subjects related to technology research. We also use the extensive library of directories and Journals on various technology domains. Our analysts use blog posts, whitepapers, case studies, and other literature published by major technology vendors, online experts, and industry news publications.

Inputs from Industry Participants

Quadrant analysts collect relevant documents such as whitepapers, brochures, case studies, price lists, datasheet, and other reports from all major industry participants.

Primary Research

Quadrant analysts use a two-step process for conducting primary research that helps us in capturing meaningful and most accurate market information. Below is the two-step process of our primary research:

Market Estimation: Based on the top-down and bottom-up approach, our analyst analyses all industry participants to estimate their business in the technology market for various market segments. We also seek information and verification of client business performance as part of our primary research interviews or through a detailed market questionnaire. The Quadrant research team conducts a detailed analysis of the comments and inputs provided by the industry participants.

Client Interview: Quadrant analyst team conducts a detailed telephonic interview of all major industry participants to get their perspectives of the current and future market dynamics. Our analyst also gets their first-hand experience with the vendor's product demo to understand their technology capabilities, user experience, product features, and other aspects. Based on the requirements, Quadrant analysts interview with more than one person from each of the market participants to verify the accuracy of the information provided. We typically engage with client personnel in one of the following functions:

- Strategic Marketing Management
- Product Management
- Product Planning
- Planning & Strategy

Feedback from Channel Partners and End Users

Quadrant research team research with various sales channel partners, including distributors, system integrators, and consultants to understand the detailed perspective of the market. Our analysts also get feedback from end-users from multiple industries and geographical regions to understand key issues, technology trends, and supplier capabilities in the technology market.

Data Analysis: Market Forecast & Competition Analysis

Quadrant's analysts' team gathers all the necessary information from secondary research and primary research to a computer database. These databases are then analyzed, verified, and cross-tabulated in numerous ways to get the right picture of the overall market and its segments. After analyzing all the market data, industry trends, market trends, technology trends, and key issues, we prepare preliminary market forecasts. This preliminary market forecast is tested against several market scenarios, economic scenario, industry trends, and economic dynamics. Finally, the analyst team arrives at the most accurate forecast scenario for the overall market and its segments.

In addition to market forecasts, our team conducts a detailed review of industry participants to prepare competitive landscape and market positioning analysis for the overall market as well as for various market segments.

SPARK Matrix: Strategic Performance Assessment and Ranking

Quadrant Knowledge Solutions' SPARK Matrix provides a snapshot of the market positioning of the key market participants. SPARK Matrix representation provides a visual representation of market participants and provides strategic insights on how each supplier ranks in comparison to their competitors, concerning various performance parameters based on the category of technology excellence and customer impact.

Final Report Preparation

After finalization of market analysis and forecasts, our analyst prepares necessary graphs, charts, and table to get further insights and preparation of the final research report. Our final research report includes information including market forecast; competitive analysis; major market & technology trends; market drivers; vendor profiles, and such others.