IDC MarketScape

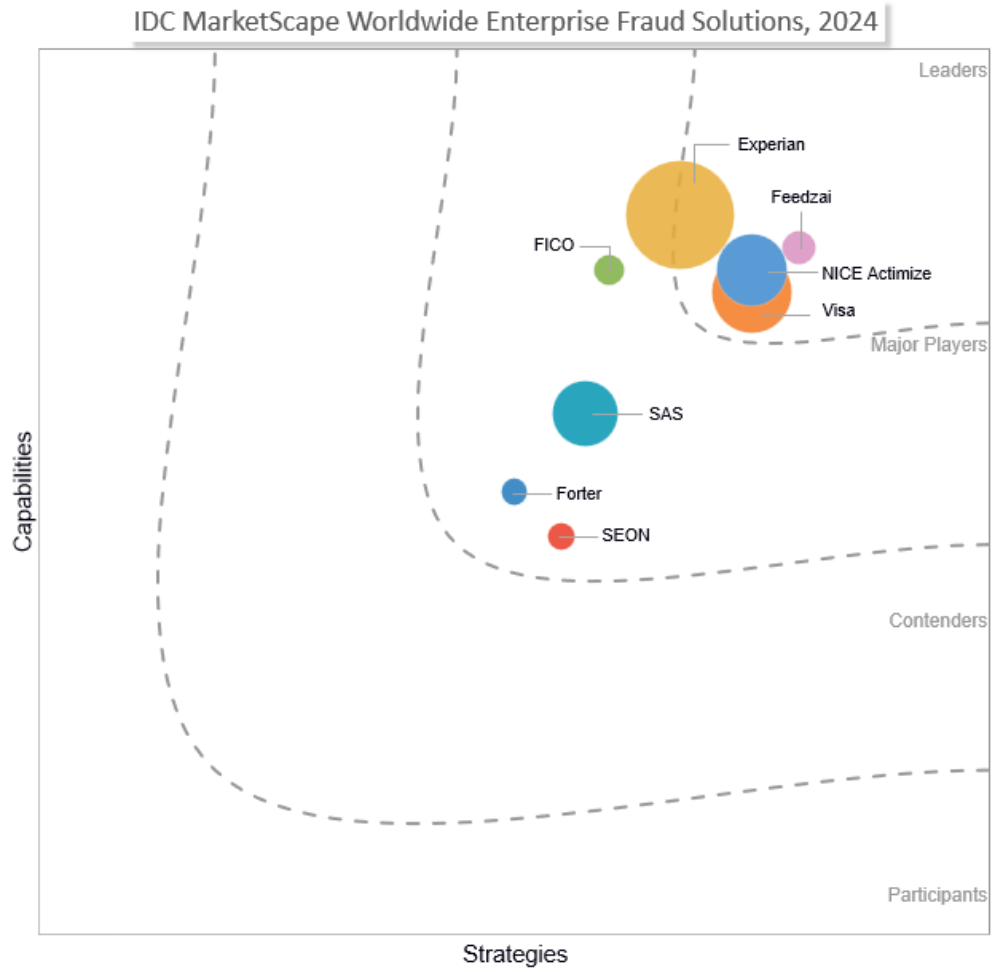
IDC MarketScape: Worldwide Enterprise Fraud Solutions 2024 Vendor Assessment

Sean O'Malley

IDC MARKETSCAPE FIGURE

FIGURE 1

IDC MarketScape Worldwide Enterprise Fraud Solutions Vendor Assessment



Source: IDC, 2024

March 2024, IDC #US51939124

Please see the Appendix for detailed methodology, market definition, and scoring criteria.

IDC OPINION

The marketplace for fraud risk management solutions has been growing in recent years, as the payments types and payment methods have expanded due to growing numbers of online retailers and financial technology companies that are involved in the payments process. Along with an expanding number of companies that are exposed to fraud risk, there are also significant enhancements in technological capabilities, particularly with respect to cloud computing, which has experienced a significant increase in implementation and use, particularly within the financial services industry. This combination of factors is driving some significant changes in the fraud risk vendor solution marketplace.

Some newer fraud solutions have been developed with an eye toward the online payments' world, and many are taking advantage of the increased computing power that is available to both expand the data sets being used to identify potential fraud incidents and enhance the models designed to detect, mitigate, and prevent fraud.

While fraud incidents have always existed, the increasing use of no-contact, online, and remote financial transactions and customer onboarding has increased fraud loss amounts during the COVID-19 era and continue today. The U.S. Federal Trade Commission (FTC) tracks and reports on fraud scam incidents and loss amounts each year. The dollar losses associated with those fraud scam losses reported by the FTC continues to increase, rising to $10 billion in losses reported by fraud scam victims in 2023. Many businesses and financial institutions also report that fraud losses, from all fraud types (not just fraud scam losses), are continuing to increase, motivating many of them to seek fraud risk management solutions that can help contain, and hopefully reduce, fraud loss amounts and fraud incidents.

IDC MARKETSCAPE VENDOR INCLUSION CRITERIA

Vendor inclusion criteria includes the following three criteria:

- Vendor offers either a standalone fraud solution or a fraud solution that is included with additional functionality but must include the capability of identifying suspected fraud incidents (either through fraud rules, typologies, and fraud models or through artificial intelligence [AI]), providing case management for the dispositioning of the suspected fraud incident (or alert), and reporting capabilities for the purposes of management oversight.
- Vendor must offer the fraud solution to banks (or credit unions) in at least one global region (Europe, United States [or North America], Asia/Pacific, or Latin America).
- Vendor must have at least 10 active client implementations of their fraud solution.

ADVICE FOR TECHNOLOGY BUYERS

With regard to the marketplace for fraud solutions, there are several good vendor alternatives to consider; however, some of the important considerations from a functional perspective deal with the types of financial products that each vendor might focus on. There are certain fraud solutions that are more appropriate for the types of fraud experienced with credit cards, others that focus more on online payments and online merchants, and others that are used for a broader range of financial products

and financial institution types. It depends on the buyer's needs, based on the potential fraud types and financial products that are most relevant to their business, to select which fraud solution is best suited to help identify, mitigate, and prevent fraud losses experienced by the business based on their fraud risk profile.

Other considerations include whether the detection and prevention of potential fraud in real time, and prior to the completion of a financial transaction, is a necessity or priority. Many solutions are increasingly moving toward real-time fraud detection and prevention, but it's important to evaluate each vendor's capabilities in this area in the evaluation and vendor selection process.

For those technology buyers requiring the broadest range of financial product coverage and would benefit those most from assistance designed to aid the technology buyer in the model development and model enhancement process, perhaps it would be wise to consider a fraud solution that has both artificial intelligence and machine learning (ML) capabilities. These capabilities can provide significant assistance to the buyer in terms of expanding data sets used in the fraud risk model development process and reducing the time and effort involved in making enhancements to the fraud risk models used in production.

VENDOR SUMMARY PROFILES

This section briefly explains IDC's key observations resulting in a vendor's position in the IDC MarketScape. While every vendor is evaluated against each of the criteria outlined in the Appendix, the description here provides a summary of each vendor's strengths and challenges.

Experian

Experian is positioned in the Leaders category for the 2024 IDC MarketScape for enterprise fraud solutions. The company was started as part of Credit Data Corporation, which was purchased by TRW in 1968 and then spun off by TRW as Experian in 1996. Experian is a credit rating agency, alongside competitors Equifax and TransUnion. Its CrossCore fraud solution was evaluated for this IDC MarketScape document.

Strengths

Experian's CrossCore product is designed to help mitigate fraud while maintaining a positive customer experience with an integrated set of identity protection and fraud prevention solutions. CrossCore is a cloud-based platform and workflow orchestration engine that gives clients the ability to apply user-selected data and fraud mitigation tools with data orchestration. It is capable of providing advanced analytics using machine learning, based on a combination of Experian's proprietary and partner data to return a decision. Experian has credit data on over 1.5 billion consumers and over 200 million businesses.

In addition to evaluating the transactional data for potential fraud, Experian's CrossCore solution includes identity-authentication tools. The solution uses identity data, device intelligence, email and phone intelligence, alternative identity data, biometrics, behavioral biometrics, one-time passwords, and document verification to confirm identities and aid with identity protection, including synthetic identity protection. Experian utilizes multiple data partnerships in its fraud solution, which often can help provide a more comprehensive understanding of fraud risks and exposures.

CrossCore is designed to address multiple fraud typologies, including the following: account opening, account takeover, bust-out fraud, commercial entity fraud, first- and third-party fraud, authorized push payment (APP) fraud, money laundering, and mule accounts.

Challenges

Experian, as a credit rating agency, is focused primarily on credit-based decisions, which influences the focus of the CrossCore fraud solution. While it mitigates fraud at account opening and account takeover, CrossCore's transaction risk scoring focuses primarily on credit and debit card transactions at the point of sale for online merchants and banks (rather than bank account transactions).

Feedzai

Feedzai is positioned in the Leaders category for the 2024 IDC MarketScape for enterprise fraud solutions. Feedzai was founded in 2011 as a data science company that develops real-time machine learning tools to identify fraudulent payment transactions.

Strengths

Feedzai is designed to be omni-channel, enabling its fraud solution to monitor different customer interaction methods. Feedzai utilizes real-time customer interaction and transaction data to increase accuracy and improve the customer experience.

The risk scoring process used by Feedzai is based on behavioral and transactional patterns that continuously learn and evolve over time, which is beneficial given the nature of fraud typologies to change rather quickly. Users of the Feedzai fraud solution can also adjust parameters and thresholds to better align with the business risk appetite of their financial institution.

The Feedzai fraud solution can also adjust fraud countermeasures with rules and machine learning models that can leverage data across all channels and geographies, enabling either a globally consistent approach or a regionally tailored approach to fraud prevention.

Feedzai received the best rating from customers regarding total cost of ownership, possibly due to the contract option that structures part of Feedzai's compensation to be based on a proportion of the reduction in fraud losses by using Feedzai's fraud solution. This innovative approach to pricing its fraud solution may attract additional customers and provide a competitive edge.

Challenges

Feedzai is still a growing player in the fraud solutions business space, working to expand its customer base. Gaining market share competing, in some instances, with fraud solution vendors that are larger and more established will be challenging.

FICO

FICO is positioned in the Major Players category for the 2024 IDC MarketScape for enterprise fraud solutions. Fair Isaac Corp. (FICO), founded in 1956 and active in a broad range of industries, is an analytics company most commonly associated with the production of personal credit ratings, also known as "FICO scores," which are used as a common measure of a personal creditworthiness by multiple types of financial services companies. FICO Falcon Intelligence Network is the core of the enterprise fraud solution currently offered by FICO, a company that has had an enterprise fraud solution since 1992.

Strengths

FICO Fraud Solution conducts real-time transaction analysis and is designed to work across multiple channels. Fraud Manager is also designed to be deployed out of the box, making the rollout and implementation of the solution relatively easy and quick. The fraud prevention models used by FICO Fraud Solution rely on artificial intelligence and machine learning and can be customized to target specific portfolios as well as geographic regions. FICO has over 100 patents in AI and ML.

FICO Fraud Solution uses data from more than 10,000 financial institutions to design models to address both global and regionally specific fraud trends. The Fraud Solution has patented analytic technology covering fraud risks in credit cards, debit cards, prepaid cards, commercial cards, and digital payments (e.g., Zelle, Venmo, and FedNow+).

The functionality of FICO Fraud Solution enables business and financial users to define, test, and deploy anti-fraud rules based on their organization's requirements and strategies with the solution's rules engine.

Challenges

While FICO Fraud Solution is the latest from a company that has been in fraud identification and prevention for a long time, the solution has continued to be expanded and improved over time. At this point, the functionality is designed to be used by so many different business functions that the learning curve can be quite steep.

Forter

Forter is positioned in the Major Players category for the 2024 IDC MarketScape for enterprise fraud solutions. Forter was founded in 2013 and is a software-as-a-service (SaaS) company, offering real-time fraud detection and prevention, identity verification, and payment optimization services.

Strengths

Forter's fraud analytics have been used to conduct fraud decisions on over $1 trillion of online transactions, primarily for online retailers. Forter also uses the 1.2+ billion identities from its cross-merchant data set to conduct analysis of customer behavior and buying patterns to help identify potentially anomalous transaction activity for fraud. Forter is designed to provide users with information to make accurate, real-time decisions about every digital interaction. Forter claims to be powered by the largest network of online retailers.

Forter claims that its fraud solution has reduced chargebacks and false declines by up to 90% and enables instant fraud decisioning. The company claims its fraud solution is useful in the optimization of payments, enabling fewer declines for transactions while reducing fraud rates, thus positively impacting profitability for those companies using Forter.

Challenges

Forter is focused primarily on digital transactions, and the primary product focus is for card transactions involving customer purchases. At this time, the majority of companies using Forter are online retailers, so the primary challenge for Forter going forward is the expansion into other transaction types or more expanded use within financial services.

NICE Actimize

NICE Actimize is positioned in the Leaders category for the 2024 IDC MarketScape for enterprise fraud solutions. NICE was founded in 1986 as Neptune Intelligence Computer Engineering. NICE Actimize is a subsidiary of NICE (Actimize was acquired in 2007), which focuses on innovative financial crime technologies to protect institutions and consumers. NICE Actimize deals with real-time fraud prevention, anti-money laundering (AML) detection, and trade surveillance solutions.

Strengths

NICE Actimize is the fraud solutions vendor of choice for nearly all the largest banks, across all regions, which makes it one of the most widely used fraud solutions, NICE Actimize uses artificial intelligence and machine learning to develop and improve fraud prevention models and methodologies. However, NICE Actimize has conducted analysis to confirm that machine learning alone is not enough to optimize fraud prevention. It needs to be augmented with fraud expertise, which is why the IFM Enterprise Fraud Management solution also has a library of expert fraud features, developed by Actimize's experts – to help maximize the detection rate with the minimum alert rate and enable more rapid time to value for its customers.

NICE Actimize has approximately 80 data partners globally, which help provide the IFM Enterprise Fraud Management solution with an expanded data set from which to develop fraud prevention models.

NICE Actimize's IFM Enterprise Fraud Management platform enables customers to leverage collective intelligence and cross-industry expertise accumulated by NICE Actimize to protect its customers, avoid reputational damage, and safeguard financial institutions. This enables all financial institutions using IFM to benefit from what other financial institutions using the solution have learned and are learning, as new fraud typologies emerge and change.

NICE Actimize is in the process of launching its next-generation IFM (version 11) designed to use AI across the life cycle of fraud management with the goal of making fraud prevention teams more accurate, agile, and efficient. Capabilities will include intelligent orchestration, network analytics, and alert and case management powered by GenAI.

As NICE Actimize looks to expand its customer base with more midsize institutions, there is another platform, Xceed, which is intended to be appealing to this customer base.

Challenges

Some financial institutions that evaluate NICE Actimize as a potential fraud solution are of the opinion that the total cost of ownership is priced at a premium.

SAS

SAS is positioned in the Major Players category for the 2024 IDC MarketScape for enterprise fraud solutions. As a leader in analytics, SAS Institute was founded in 1976 and is active in a broad range of industries, including financial services. The SAS Fraud solution uses industry-leading data analytics and machine learning designed to be part of a full-service, integrated offering. However, SAS Fraud solution can also be purchased as a standalone application and integrated with other (non-SAS) software solutions.

Strengths

SAS has a strong track record with respect to machine learning analytics, which is one of the key components of its success with respect to the detection and prevention of fraud, as well as the company's success in the financial services industry in general. To address the data ingestion and computational requirements for the development and use of AI models that are used in combination with rules and ML analytics to conduct fraud analysis, detection, and prevention, SAS offers a cloud-native based architecture. Many clients are using the SAS Fraud solution successfully in an on-premises deployment.

SAS has a very broad range of functional choices, designed to capitalize on the solution's data analytics and AI and ML capabilities and enable users to design customized models through out-of-the-box methodologies designed to identify fraud incidents. The AI/ML-generated modeling capabilities can also be used to develop a challenger model and deploy this in combination with the user-selected champion model, into production together, as part of a robust model governance process. The SAS Fraud solution offers the user core functionality including real-time dynamic profiling and ML model scoring and decisioning.

Challenges

While the functionality of SAS' Fraud solution offers a great deal of customizable use, the options can be challenging for a first-time adopter when trying to make a selection regarding which approach will be the most productive. While the machine learning model in the SAS Fraud solution is low code (no code), the learning curve to use all of the available functionality can be quite steep. To help avoid confusion about the broad range of custom selections, the user can opt to use the AI/ML capabilities of the solution to recommend and specify model variables and methodologies.

One of the challenges also deals with the structure of the SAS Fraud solution. Users have commented that they feel there is not enough customization of the solution. This may be in part a compromise to ensure cost-effective deployments for SAS to implement rather than design customizations of its solution for a single user or limited number of users. The current version of the SAS Fraud solution has a wide variety of functional choices available to the user.

Some users that have evaluated the SAS Fraud solution believe the total cost of ownership is higher than other solutions they evaluated.

SEON

SEON is positioned in the Major Players category for the 2024 IDC MarketScape for enterprise fraud solutions.

SEON was founded in 2018 and, as such, is a relatively new company in the enterprise fraud solution space. Because of being a recent entrant in the fraud solution business space, SEON is still in the process of refining and executing its strategy, developing strategic partnerships that can help the company grow and succeed.

SEON is focused on real-time fraud detection by analyzing transactional data, using artificial intelligence and machine learning to detect anomalies that may be indicative of fraud.

Strengths

As a new company, SEON has an advantage in that it doesn't need to replace its rules-based fraud detection system, which is how many of the initial vendors in the fraud solution space started. SEON did not begin the solution development in an environment where data availability and computing power were significant business constraints. As a result, SEON was able to build its solution to enable systems integration.

SEON's data analytics is based on using artificial intelligence and machine learning to analyze transactional data for potential indications of fraud.

Challenges

SEON is still a relative newcomer into a business space where other companies have been in for decades. Vying for market share and competing against other fraud solutions providers that are more dominant players and more established vendors will be challenging as SEON seeks to expand and grow. SEON would also benefit from additional data partners, capable of providing their fraud solution with more information, so as to enable the development of better fraud prevention models.

Visa

Visa is positioned in the Leaders category for the 2024 IDC MarketScape for enterprise fraud solutions. Visa was established in 1958 by Bank of America and is one of the largest multinational payment card services companies. Visa acts primarily as a credit card issuer and payment platform and conducts fraud management. Visa Risk Manager, the enterprise fraud solution, is involved in analyzing a very large amount of transaction volume ($691 billion in 2021) to identify potential fraud incidents.

Strengths

The volume of transactions, and transaction data, that is processed involving Visa, provides an advantage to Visa Risk Manager in detecting and identifying fraud incidents and typologies. Certain fraud typologies are sometimes challenging to identify when viewing a small segment of the transactional data. It is easier to identify, and quantify, fraud typologies and their impact by analyzing a large segment of the transactional data, which is the advantage that Visa has due to the large amount of transactional volume analyzed by Visa Risk Manager.

Visa Risk Manager uses complex analytics and tools, including artificial intelligence and machine learning, to analyze the large data set for potential fraudulent transactions, but it also provides the user, in real time, with a risk score, from 1 to 99, designed to reflect the level of perceived risk associated with a transaction. The measured uptime for Visa Risk Manager is 99.9999%, according to VisaNet Authorization Performance Data, which indicates that the solution is highly reliable with virtually no downtime.

In terms of measurable business impact, Visa claims to have prevented $29 billion in fraud from July 1, 2022, to June 30, 2023.

Challenges

Because of the focus on payment card services, most of the fraud detection efforts for Visa focus on payments, primarily those payments dealing with credit cards. While Visa Risk Manager is well suited for this purpose, only the future will tell if this solution can extend to a broader range of financial products.

APPENDIX

Reading an IDC MarketScape Graph

For the purposes of this analysis, IDC divided potential key measures for success into two primary categories: capabilities and strategies.

Positioning on the y-axis reflects the vendor's current capabilities and menu of services and how well aligned the vendor is to customer needs. The capabilities category focuses on the capabilities of the company and product today, here and now. Under this category, IDC analysts will look at how well a vendor is building/delivering capabilities that enable it to execute its chosen strategy in the market.

Positioning on the x-axis, or strategies axis, indicates how well the vendor's future strategy aligns with what customers will require in three to five years. The strategies category focuses on high-level decisions and underlying assumptions about offerings, customer segments, and business and go-to-market plans for the next three to five years.

The size of the individual vendor markers in the IDC MarketScape represents the market share of each individual vendor within the specific market segment being assessed.

The MarketScape graph is designed to illustrate where each fraud risk vendor, based on input from customers, ranks relative to each other with respect to strategy and capabilities. Customer input used in this MarketScape was provided by customers selected by the fraud risk solution vendor and provided to IDC in a structured discussion where each customer was asked their opinion and rating with respect to several aspects of the fraud vendor solution that were then used in the scoring of the vendor capabilities.

Keep in mind that the market share, which influences the size of the circle for each vendor on the MarketScape graph, is based on the revenue of each vendor. Since fraud risk solution-specific revenue were not publicly available for all vendors, for some vendors, the company revenue was used to represent market share. This means that the graphic representation of market share by vendor is not necessarily representative of their specific market share in the fraud risk vendor space.

IDC MarketScape Methodology

IDC MarketScape criteria selection, weightings, and vendor scores represent well-researched IDC judgment about the market and specific vendors. IDC analysts tailor the range of standard characteristics by which vendors are measured through structured discussions, surveys, and interviews with market leaders, participants, and end users. Market weightings are based on user interviews, buyer surveys, and the input of IDC experts in each market. IDC analysts base individual vendor scores, and ultimately vendor positions on the IDC MarketScape, on detailed surveys and interviews with the vendors, publicly available information, and end-user experiences in an effort to provide an accurate and consistent assessment of each vendor's characteristics, behavior, and capability.

Market Definition

For this research, IDC defines this market as solutions designed to identify (often through the use of fraud rules, typologies, fraud models, or artificial intelligence), provide case management, resolve, track status, and report on suspected fraud incidents within a bank.

Strategies and Capabilities Criteria

Strategies criteria includes evaluating vendors based on their cloud-based delivery, local versus global resources for delivery, adjacent portfolio growth, growth of customer base, customer assessment of vendor's innovation, customer assessment of vendor's overall research and development strategy, functionality or offering strategy with respect to matching evolving customer's business needs, and the vendor's track record in achieving road map strategic objectives.

Capabilities criteria includes evaluating vendors based on their customer's satisfaction with respect to client relationship and account management, functionality or offering with respect to predictive analytics, total cost of ownership of product/offering to IT buyer/user, collection of fraud data, functionality or offering with respect to essential capabilities, and cost-effectiveness (actual licensing subscription fees versus value and vendor's relationships with fraud data providers).

Tables 1 and 2 provide key strategy and capability success measures, respectively, related to the market of worldwide enterprise fraud solutions.

TABLE 1

Key Strategy Measures for Success: Worldwide Enterprise Fraud Solutions

Strategies Criteria	Definition	Weights (%)
Functionality or offering strategy	▪ Strategic capabilities to evolve and enhance the functionality of the fraud solution offering ▪ Historical track record of achieving strategic objectives	20.0
Delivery	▪ A road map based on customer and partner input that cover part of cloud, data analysis, mobility solutions, and social integration ▪ Support resources available globally and locally for buyers	30.0
Growth	▪ Consistent growth or increase in market share ▪ Expansion of customer base by adding new customer segments	30.0
Innovation	▪ Customer assessment of vendor innovation	10.0
R&D pace/productivity	▪ Assessment of overall R&D strategy	10.0
Total		100.0

Source: IDC, 2024

TABLE 2

Key Capability Measures for Success: Worldwide Enterprise Fraud Solutions

Capabilities Criteria	Definition	Weights (%)
Functionality or offering	▪ Has a pricing model for different types of delivery, such as cloud, on premises, per user, and enterprise ▪ Evaluation of essential capabilities	25.0
Customer satisfaction	▪ Demonstrates its ability to offer specific capabilities listed ▪ Customer satisfaction assessment	20.0
Other capabilities	▪ Gathering of data from users to help guide fraud typologies and model development ▪ Relationships with fraud data vendors to help guide fraud typologies and model development	20.0
Total cost of ownership of product/offering to IT buyer/user	▪ Total cost of ownership ▪ Cost-effectiveness of solution, as assessed by customers	35.0
Total		100.0

Source: IDC, 2024

LEARN MORE

Related Research

- *IDC FutureScape: Worldwide Banking 2024 Predictions* (IDC #US51290623, October 2023)

Synopsis

This IDC study analyzes and evaluates several of the leading fraud risk management solution providers on the basis of their strategy and capabilities. Vendor strategy has been evaluated based on factors influencing the business strategy being pursued by each vendor and the perception of each vendor's customers with respect to their opinion of how successful that strategy is in addressing the fraud risk management concerns of each customer. Vendor capabilities have been analyzed based on those factors deemed to be influencing each vendor's fraud risk management solution capabilities. Customer opinion with respect to vendor capabilities has been considered with respect to the ratings provided to each fraud risk management solution vendor in the capabilities evaluation process.

"As fraud risk losses continue to increase, the pursuit of fraud risk management solutions designed to identify, mitigate, and prevent fraud incidents and losses is a topic with increasing focus within financial services." – Sean O'Malley, research director, IDC Financial Insights: Worldwide Compliance, Fraud and Risk Analytics Strategies

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets. With more than 1,300 analysts worldwide, IDC offers global, regional, and local expertise on technology, IT benchmarking and sourcing, and industry opportunities and trends in over 110 countries. IDC's analysis and insight helps IT professionals, business executives, and the investment community to make fact-based technology decisions and to achieve their key business objectives. Founded in 1964, IDC is a wholly owned subsidiary of International Data Group (IDG, Inc.).

Global Headquarters

140 Kendrick Street
Building B
Needham, MA 02494
USA
508.872.8200
Twitter: @IDC
blogs.idc.com
www.idc.com