IDC MarketScape

IDC MarketScape: Worldwide Enterprise Fraud Management in Banking 2020 Vendor Assessment

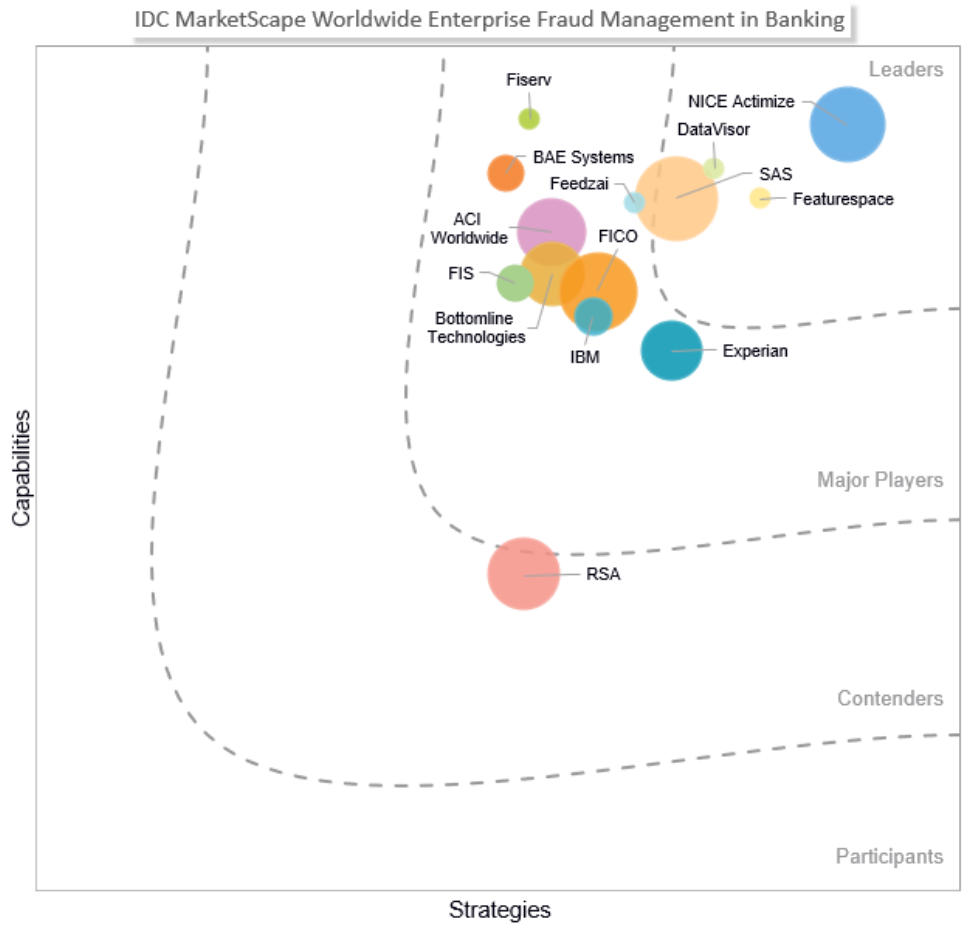
Steven D'Alfonso

THIS IDC MARKETSCAPE EXCERPT FEATURES BOTTOMLINE TECHNOLOGIES

IDC MARKETSCAPE FIGURE

FIGURE 1

IDC MarketScape: Worldwide Enterprise Fraud Management in Banking Vendor Assessment



Source: IDC, 2020

July 2020, IDC #US45617020e

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

IN THIS EXCERPT

The content for this excerpt was taken directly IDC MarketScape: Worldwide Enterprise Fraud Management in Banking 2020 Vendor Assessment (Doc # US45617020). All or parts of the following sections are included in this excerpt: IDC Opinion, IDC MarketScape Vendor Inclusion Criteria, Essential Guidance, Vendor Summary Profile, Appendix and Learn More. Also included is Figure 1.

IDC OPINION

This IDC Financial Insights study presents a 2020 vendor assessment of worldwide enterprise fraud management (EFM) technology providers. This research quantitatively and qualitatively assesses multiple characteristics that help explain a technology supplier's success and position in the marketplace relative to its peers. This evaluation is based on a standardized set of parameters from which IDC can produce a comparative analysis of enterprise fraud management technology providers.

Banking institutions worldwide are recognizing the need to holistically manage fraud risk. This means having the ability to understand a customer's or entity's behavior across channels and lines of business. The siloed nature of legacy systems as well as the implementation of channel-specific fraud applications inhibits a bank's ability to understand an entity's fraud risk in total. Banks should consider fraud as a strategic priority within the overall digital transformation strategy of the organization. Too often, fraud is viewed as a bottom-line expense. Forward-looking banks view fraud management as an important component of managing the customer experience, leveraging fraud analytics to enhance product and service offerings.

The growth of digital and mobile banking as well as expanding ecommerce and digital payments necessitates that banks can identify potential fraud in real time. In addition, they must be agile enough to quickly adapt to changing fraud threats and trends, identify suspicious activity across channels, and detect organized ring activity.

Internal fraud and abuse (aka occupational fraud) prevention and detection are important in most organizations but are acutely important in banking as hundreds to thousands of employees have access that would allow them to misappropriate money. The Association of Certified Fraud Examiners in its 2020 Report to the Nations noted that occupational fraud is a worldwide issue. Its report further noted that the median loss was $125,000 per occupational fraud case in its study. However, cases that were detected by active employee surveillance/monitoring resulted in median losses of just $44,000 and were detected 50% sooner than the 14-month median duration for occupational fraud cases. All the vendors in this study have the analytical capabilities to employ internal fraud monitoring; however, just over half of them have bank customers using their applications for internal fraud detection. (For more information, see the Consider When Summary section.)

IDC MARKETSCAPE VENDOR INCLUSION CRITERIA

This study includes 14 worldwide providers of EFM applications and platforms. The vendors included in this study are all substantial competitors within the retail banking fraud management space. To be included within this study, vendors must provide their solution in multiple worldwide regions and have at least 25 active customers in at least two regions (North America, EMEA, Latin America, and APAC).

Other technology providers were considered for inclusion in this assessment but did not meet the evaluation criteria.

Research Scope and Definitions

The intent of this study was to profile and assess providers of enterprise fraud management technology on a worldwide scale. The term *enterprise fraud management* can be interpreted differently by different people. IDC Financial Insights is providing the following definition and scope statements to help clarify what was considered within this study.

Scope

The scope included an assessment of software vendors that offer fraud prevention technologies designed for use in the retail banking segment. The vendor applications should provide solutions for fraud related to new accounts, deposits, payments, transfers, online and mobile banking, and insider fraud and abuse.

The scope excluded card fraud, mortgage, and other loan-related fraud.

Definitions

- **Enterprise fraud management:** For purposes of this study, IDC defines enterprise fraud management as the ability to identify and prevent external and internal fraud across all processes, channels, users, and transaction types within a financial institution (FI). EFM tools enable FIs to analyze behavior; connect people, places, things, and entities; and identify complex criminal activity to identify suspicious or unusual activity across all channels.
- **Internal fraud and abuse:** For purposes of this study, IDC defines internal fraud to include activities of employees to circumvent internal controls, policies, and regulations to engage in misappropriation of company or customer funds or other corrupt activities. In addition, internal fraud includes employees collaborating with external bad actors to commit fraud against the company or its customers.

ADVICE FOR TECHNOLOGY BUYERS

IDC Financial Insights offers the following guidance to financial institutions for the selection of an EFM technology provider:

- The degree to which the vendors assessed in this study are separated is not vast. Consideration should be given to all vendors regardless of position within this assessment.

  The list of vendors within this study should be viewed as a short list of potential EFM technology providers. Most of the vendors have similar baseline capabilities. The vendor profiles should guide a prospective buyer's interest in individual vendors regardless of position in this study. Also, a vendor's position in the Leader category does not equate to an ideal fit for all organizations. Bank buyers should strongly consider a vendor's strategic vision and approach to establishing effective EFM. Likewise, buyers should also consider the depth of a vendor's experience in working with retail banks and the complexities associated with fraud management in a retail banking environment.
- There is considerable commonality in capabilities and strategies across the different vendors. The areas in which IDC identified differentiation were:
  - **Model management:** Vendors with advanced capabilities provide built-in model creation, testing, and deployment. Advanced capabilities around model development also include

the democratization of data science, enabling non-IT and nontechnical staff to create machine learning (ML) models. In addition, while most vendors can upload existing bank fraud models, there was variation between vendors with respect to limitations around that capability. Furthermore, some vendors provide self-learning models that require little or no retraining.

- **Link/network analytics:** Vendors with advanced capabilities offered visual link analytics as a standard part of their offering. Vendors with this capability should also enable role-based permission controls so that fraud managers can determine who has access to the visual analytic capability.
- **Real-time detection/scalability:** All 14 vendors in this study indicated an ability to support real-time transaction fraud risk decisioning. The vendor-stated upper-limit volume processing capabilities based on transactions per second varied considerably. Buyers considering a fraud platform to support real-time fraud risk decisioning should closely examine prospective vendors in this area.
- **Internal fraud and abuse:** There are differences between the firms that have active bank customers using their platforms for internal fraud use cases. A few vendors have banks using analytics around a limited set of use cases, while others have banks employing analytics for many use cases. At least one vendor provides advanced capabilities around employee screen navigation replay.
- **Bank customer portfolio:** IDC asked about the makeup of each vendor's portfolio of retail bank customers by asset tiers. There are clear differences related to the distribution of bank sizes served by the vendors. There were a few providers that had an even, well-rounded distribution of customers across the asset tiers. There were many that had none or small numbers of customers in one or two tiers. IDC believes this is an important aspect for bank buyers to understand about prospective technology suppliers to ensure that the vendor has sufficient depth of experience working with similar-sized institutions of the buyer.
- **Staff banking domain experience:** IDC did not quantitatively assess staff industry experience in this study; however, through conversations and observations, IDC noted a difference between some firms. Several firms had mid- to senior-level employees that previously worked in fraud at a bank. All the vendors employ product managers and data scientists that are highly knowledgeable about fraud and the technology to support an EFM approach. Those vendors with experienced fraud practitioners, from banking, may have a better ability to understand the needs, requirements, and pain points of the bank buyer.

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.

Bottomline Technologies

Bottomline Technologies (BT) is positioned in the Major Players category in this 2020 IDC MarketScape for worldwide enterprise fraud management in banking.

Bottomline Technologies is a provider of payment automation technology to banks and corporate treasury functions worldwide. Its suite of products covers international payments, cash management, fraud management, and compliance.

BT's Cyber Fraud and Risk Management (CFRM) offering provides a comprehensive fraud management product set that leverages user behavior analytics as a foundational technology. Hundreds of banks worldwide use the CFRM application to manage fraud related to all fraud typologies, including a well-established insider fraud capability. In addition, the CFRM application provides a web fraud and security module to monitor web traffic and user interactions to protect bank customers' account in the online channel. The web fraud and security capability is uncommon for an enterprise fraud management provider platform.

Strengths

- Bottomline Technologies provides a unique set of capabilities through its CFRM offering.
- It has a highly flexible application; end users can configure their own displays and dashboards for their specific needs.
- Secure payments are enabled through an advanced user behavior analysis of customers' monetary and nonmonetary behavior in context. The user behavior analysis also integrates security capabilities to identify presence of malware on end-user devices as well as other device and user attributes.
- Screen-by-screen replay of user sessions is used to significantly aid alert investigation workloads.
- Bottomline Technologies provides highly explainable, self-learning machine models, which minimize model retraining efforts.
- It provides an advanced insider fraud capability with a library of configurable rules to detect anomalies in work patterns. Its user behavior analytics capabilities enable a bank to identify and prevent data exfiltration, embezzlement, and policy violations.
- The insider fraud and abuse capabilities are further enhanced through the screen-by-screen replay capability, which aids investigator efficiency in internal investigations.

Challenges

Bottomline Technologies has quietly built a solid and comprehensive enterprise fraud management offering with unique functionality. Building awareness of its CFRM offering, within the banking industry, should be an important strategy component.

Consider Bottomline Technologies When

Bottomline Technologies has CFRM implementations in tier 1 to tier 4 banks. Any bank that is seeking a flexible, agile fraud management system with unique capabilities should consider Bottomline Technologies.

Consider When Summary

Internal Fraud and Abuse Considerations

One of the qualifying criteria for this study was that each vendor must offer internal fraud and abuse capabilities. While all the vendors do have the capability to develop internal fraud models and apply analytics, not all of them have implementations in which their bank customers are using their applications for internal fraud monitoring. Although we have tried to highlight, in their individual

profiles, the vendors that have applied internal fraud use cases, we wanted to further highlight them in this section.

Any banks that are considering vendors that have targeted models for internal fraud and have a substantial portion of their customers using their technology for internal fraud should consider the following vendors:

- BAE
- Bottomline Technologies
- DataVisor
- Featurespace
- FIS
- Fiserv
- NICE Actimize
- SAS

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 market sizes are estimates based on the disclosed number of bank customers and the percentage of those customers in various asset size tiers.

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 purposes of this study, IDC defines enterprise fraud management as the ability to identify and prevent external and internal fraud across all processes, channels, users, and transaction types within a financial institution. Enterprise fraud management tools will enable financial institutions to analyze behavior; connect people, places, things, and entities; and identify complex criminal activity to identify suspicious or unusual activity across all channels, including internal fraud and abuse.

LEARN MORE

Related Research

- *IDC MaturityScape: Artificial Intelligence in Banking 1.0* (IDC #US45823120, March 2020)
- *AI-Based Automation Framework for Risk and Compliance in Financial Services* (IDC #US45710719, December 2019)
- *Securing Multi-Rail Real-Time Payments: Future of the Fraud Stack* (IDC #US45472619, September 2019)
- *Solving the $4+ Billion Problem of Synthetic Identity Fraud* (IDC #US45264619, June 2019)

Synopsis

This IDC study comparatively analyzes the enterprise fraud management capabilities and strategies of 14 worldwide fraud technology providers. The study provides retail bank buyers of enterprise fraud management platforms a short list of vendors to consider.

"In today's digital and mobile banking environment, banks should be looking to manage fraud across channels and lines of business from a single view of fraud risk. A platform that can integrate legacy channel fraud applications and point solutions to create a unified fraud risk score for any entity in real time is a strategic goal that banks should be striving to achieve." – Steven D'Alfonso, research director, IDC Financial Insights

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. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

Global Headquarters

5 Speen Street
Framingham, MA 01701
USA
508.872.8200
Twitter: @IDC
idc-community.com
www.idc.com