Aite PARTNER. ADVISOR. CATALYST.

AIM Evaluation: Fraud and AML Machine Learning Platform Vendors

MARCH 2019

Julie Conroy

TABLE OF CONTENTS

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

LIST OF FIGURES

LIST OF TABLES

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

IMPACT POINTS

- Machine learning platforms are an important technology that businesses are turning to in their fight against financial crime. These systems represent the next generation of detection and mitigation, and they provide a way for businesses to harness one of their greatest assets—their customer data—and apply custom analytics that can evolve with the rapid pace of financial crime.
- The primary goal of firms investing in machine learning platforms is to improve their ability to detect fraud or money laundering while reducing false positives, and to have analytics that can nimbly and responsively evolve with emerging attack vectors.
- Leveraging the Aite Impact Matrix (AIM), a proprietary Aite Group vendor assessment framework, this Impact Report evaluates the overall competitive position of each vendor, focusing on vendor stability, client strength, product features, and client services. A total of 18 vendors were invited to participate in the AIM evaluation, and 14 vendors agreed to be evaluated; a total of 13 appear in the AIM framework, and the report profiles the remaining vendor.
- The market is growing rapidly, with over half of the participating vendors averaging more than 10 new customers per year for the past three years.
- With 17% of deployments on the public cloud, including two Tier-1 European banks that are taking substantial portions of their detection to Amazon Web Services (AWS) and Microsoft Azure, the market is approaching a tipping point for cloud-based fraud and anti-money laundering (AML) detection deployments.
- Aite Group's spending estimates on the financial-crime-enabling market include the software license, integration, and maintenance fees. This spending estimate also includes the professional service fees associated with data integration, model building, and maintenance. Global spending on financial-crime-enabling platforms will be nearly US$1 billion by the end of 2019 and is expected to reach US$4.72 billion by the end of 2023.
- Featurespace, Feedzai, and Simility all emerged as best in class. All three vendors are among the new generation of entrants to the market and scored high marks for the completeness of their product offerings, model performance, and the firms' responsiveness and support capabilities.
- Long-standing market players FICO and SAS are joined by Brighterion as the leaders of the contenders. All of these vendors' scores have them right on the cusp of the best-in-class category.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

INTRODUCTION

Financial crime is a lucrative business for organized crime rings, terrorists, and rogue nation states. The stakes are equally high for the financial institutions (FIs), processors, retailers, and corporations that are the target of escalating attacks. Machine learning platforms are an important technology that businesses are turning to in their fight against fraud and money laundering.[1] These systems represent the next generation of detection and mitigation, and they provide a way for businesses to harness one of their greatest assets—their customer data—and apply advanced analytical techniques that can evolve with the rapid pace of financial crime.

The crowded vendor market, with similar marketing messages and promises, can make it challenging for prospective buyers to identify the best solution for their specific set of problems and use cases. This Impact Report compares and contrasts the offerings and strategies of leading vendors and highlights their primary strengths, challenges, and points of differentiation. It also explores the key trends within the machine learning platform market for fraud and AML use cases and discusses the ways in which the technology is evolving to address market needs and challenges. Finally, to help FIs, processors, and merchants make more informed decisions as they select new technology partners, the report recognizes specific vendors for their strengths in critical areas.

METHODOLOGY

Leveraging the AIM, a proprietary Aite Group vendor assessment framework, this Impact Report evaluates the overall competitive position of each vendor, focusing on vendor stability, client strength, product features, and client services. Participating vendors must have in production fraud or money laundering detection deployments in financial services, and their platforms must be able to support the deployment of customized machine learning analytics across multiple fraud or AML use cases.

Vendors were required to complete a detailed product request for information (RFI) composed of both qualitative and quantitative questions, conduct a product briefing and demo, and provide active client references. Aite Group further augmented these client reference interviews with interviews with FI executives in its network. The end result included interviews with more than 40 fraud and AML executives across five continents to gauge their satisfaction with their vendor solution(s) and to better understand key buying criteria and value drivers.

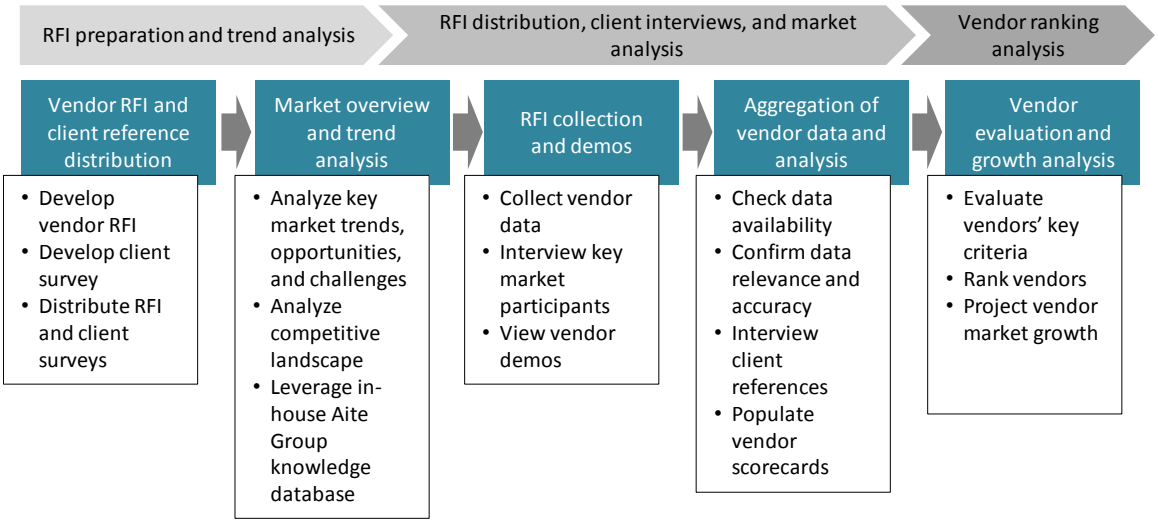
1. See Aite Group's report *Machine Learning: Fraud Is Now a Competitive Issue*, October 2017.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

AIM INTRODUCED

The AIM is a comprehensive proprietary vendor evaluation process designed to provide a holistic analysis of participating vendors and identify market leaders in each evaluated vendor market. By incorporating many aspects of a vendor's essential characteristics for success and growth, including financial and client stability, product features, and customer service, the AIM provides an actionable guide for market participants looking for viable third-party vendor solutions and services. Figure 1 highlights the key stages of the AIM methodology.

Figure 1: AIM Methodology



Source: Aite Group

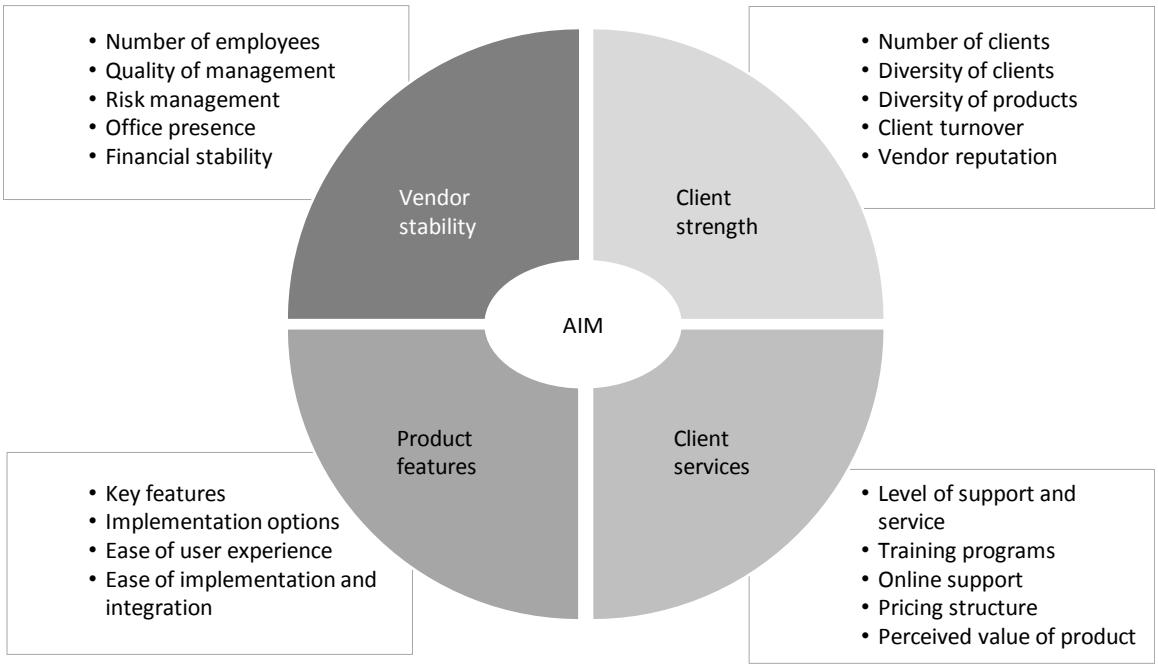
To ensure full transparency in terms of key areas of measurement and evaluation, Aite Group shares the entire AIM with each vendor prior to publication. Each participating vendor also provides client references to measure their overall satisfaction. Details of the client reference survey and questions to be discussed with clients are shared with the participating vendor prior to the interviews. Aite Group reserves the right to identify and interview other clients that may not be recommended by participating vendors to validate certain areas of analysis.

AIM COMPONENTS

The AIM is composed of four key components: Vendor stability, client strength, product features, and client services. Examples of the criteria that could be included in each component are listed in the figure below (Figure 2).

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

Figure 2: AIM Key Components



Source: Aite Group

VENDOR STABILITY

The vendor stability component evaluates the overall strength of the vendors in terms of financial stability, management reputation, risk management, and global presence. This component determines whether a given vendor has the basic foundation to compete and sustain its overall market presence.

CLIENT STRENGTH

The client strength component focuses on the number and diversity of customers for vendors, vendor reputation among the clients, and overall customer turnover. This component measures whether a given vendor has a strong foundation of clients and a robust client pipeline to sustain its growth trajectory.

PRODUCT FEATURES

The product features component analyzes the key features and functionality of vendor solutions and services, including implementation options, user experience, and the strength of the future product roadmap. This component measures whether the vendor offers enough key features and functionality to remain competitive.

CLIENT SERVICES

The client services component evaluates the pricing structure and its various attributes as well as the comprehensive nature of the vendor's client support and service infrastructure. This component measures whether the vendor provides robust service and support to provide real value to the clients.

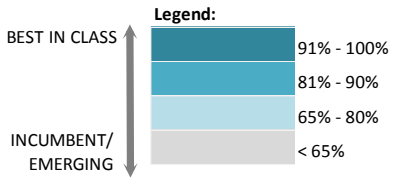
101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

AIM

After a comprehensive analysis, Aite Group can assess participating vendors within the four key evaluation components (Figure 3).

Figure 3: Sample Assessment via Heat Map Representation

Vendors	Vendor stability	Client strength	Client service	Product features
Vendor 1	81%	65%	81%	84%
Vendor 2	69%	70%	83%	88%
Vendor 3	86%	61%	81%	88%
Vendor 4	89%	91%	92%	91%
Vendor 5	81%	74%	92%	82%
Vendor 6	86%	96%	81%	82%
Vendor 7	78%	78%	92%	90%
Vendor 8	89%	87%	81%	84%
Vendor 9	69%	61%	89%	88%
Vendor 10	86%	74%	75%	85%



Source: Aite Group

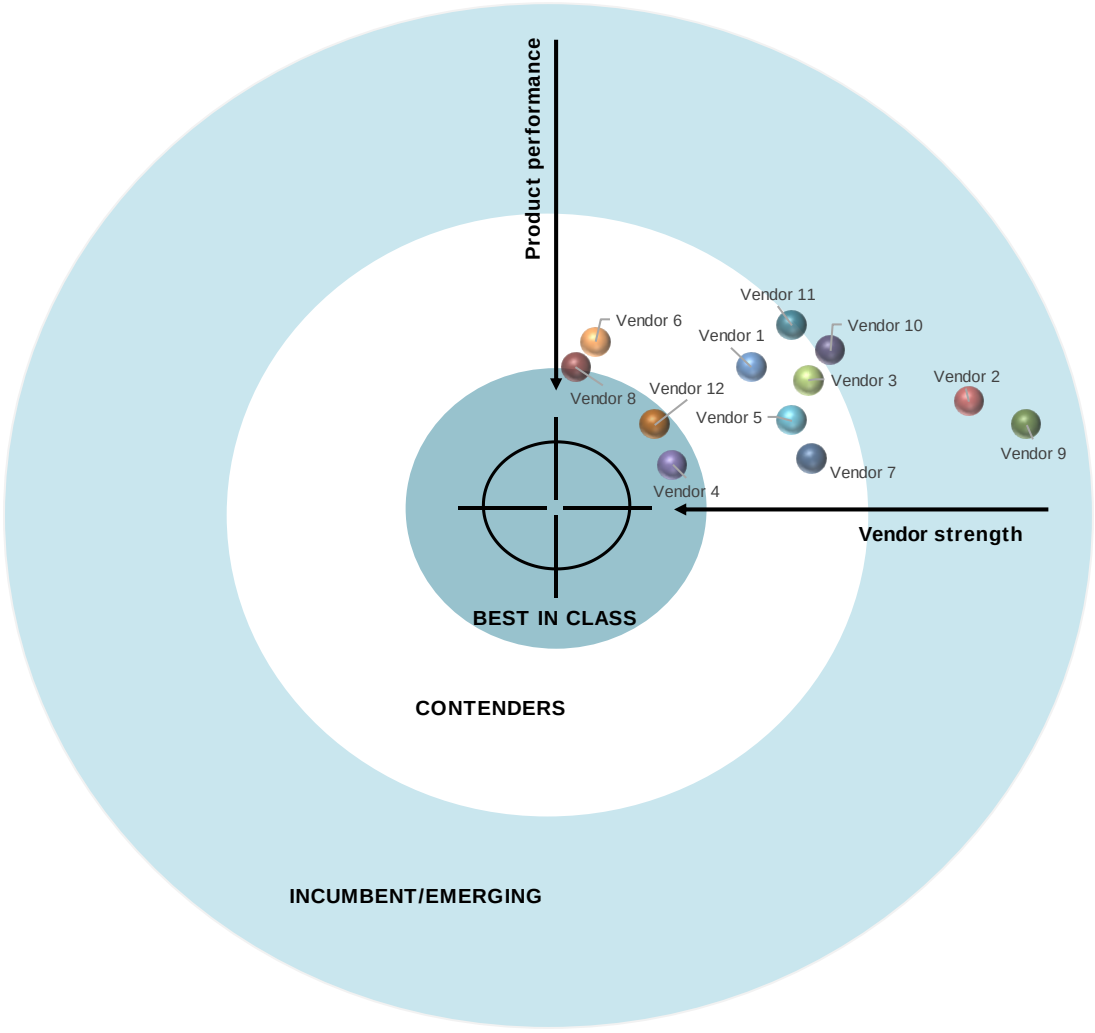
The AIM leverages these four components to create a concise composite evaluation that identifies market-leading vendors:

- **Vendor strength:** Combining the scores from the vendor stability and client strength, this criterion measures the vendor's overall long-term business viability as a product and service provider.
- **Product performance:** Combining the scores from the product features and client service components, this criterion measures the vendor's ability to deliver key product functionality and support.

Figure 4 provides a sample output of the AIM, presenting those market-leading vendors that provide robust product performance as well as showcase their ability to execute on their long-term strategies.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

Figure 4: Sample AIM



Source: Aite Group

The AIM highlights three specific types of vendor groupings as a result of the analysis:

- **Best in class:** Vendors in this grouping represent the leaders in the particular vendor market, with strong financials, diverse client bases, and robust product offerings with industry-leading functionality and reliable client service. These are essentially the leading vendors that everyone else is chasing.
- **Contenders:** Contenders have created stable businesses and client bases as well as competitive product offerings. But they struggle at times to identify the next big market trend or product features, or lack consistent research and development (R&D) or IT investment, leading to a failure to update overall performance and infrastructure. Contenders' overall competitive positions will vary a bit, from vendors that are having a tough time keeping up with the best-in-class vendors—due to a lack of resources or stable but outdated technology stacks—to vendors that

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

are just inches away from joining the best-in-class grouping if only they could properly execute on the next release or successfully capture a new client segment.

- **Incumbent or emerging:** This last grouping represents vendors that either have a large potential for future growth or are established vendors with stagnating offerings. This group may represent startups or vendors with limited resources. They may exhibit unstable business models, low client count, and limited client service capabilities. However, this group of vendors may also support innovative product features and transformative business models that will help them home in on the AIM framework.

The relative positions of vendors that have been bucketed into these three distinctive vendor groupings within the AIM are, of course, not static. In fact, an emerging vendor of today may, given the speed of innovation in recent years, find itself in the best-in-class grouping five years from now.

The beauty of the AIM is that by leveraging this framework, Aite Group analysts can pinpoint vendors' strengths and weaknesses, and vendors can utilize this framework to make sure they are on the right path to reaching the coveted best-in-class position. The flexibility of the AIM is also designed to be beneficial for those financial institutions looking to make vendor decisions tied to their unique set of internal requirements.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

THE MARKET

Organized crime rings, fueled by more than 14.7 billion data records lost or stolen since 2013,[2] are diligently targeting businesses and consumers with sophisticated fraud attacks. The trajectory of these attacks continues to increase, since the rewards are lucrative and there is very little in the way of adverse consequences. These same crime rings are often involved in complex money laundering schemes, along with terrorists, drug cartels, and rogue nation states. As a result, regulatory expectations for AML controls continue to increase—the EU's fifth AML Directive, the U.S. Federal Financial Institutions Examination Council's beneficial ownership requirements, and New York's Department of Financial Services 504 regulation are just a few examples of the rising bar of regulatory expectations for compliance.

A key challenge for fraud and AML executives is that even as the threat environment continues to escalate, FIs and retailers alike are under intense competitive pressure to enable frictionless banking and commerce experiences. In the face of this contradictory set of mandates, many businesses are looking for better solutions to help keep pace with the rapidly changing landscape. The ability to do so is increasingly a competitive differentiator for those businesses that can effectively address fraud and AML issues while keeping customer friction to a minimum.

In the '90s and early 2000s, enterprise risk management platforms hit the market with technology designed to address this challenge. These systems enabled firms to ingest customer and/or transactional data, apply rules and some analytics, enable workflows to prioritize alert triage and case management, and automate suspicious activity report filings and feedback loops. While effective, these systems have a heavy client-software footprint, making upgrades arduous, expensive, and time-consuming tasks. The data schema is typically rigid, relying on relational databases and fixed schemas, and the models in the early iterations of these engines were fairly static and reliant on model refreshes from the vendor. As a result of these factors, clients tend to be multiple versions behind due to the upgrade expense, and false positives are often higher than optimal, given the reliance on rules and periodic model refreshes.

A new breed of technology is gaining steam, which addresses many of the pain points of the prior generation. These engines enable businesses to harness internal and external data and apply advanced, iterative analytics to detect fraud and money laundering across a variety of use cases.[3] As the market experiences the promising results, the vendor space has grown rapidly, with a multitude of vendors offering solutions. Some are longtime incumbent solution providers that have added adaptive machine learning capabilities to existing platforms. They are joined by a number of new vendors that have the advantage of building from the ground up on the latest technology, but whose expertise with fraud and AML use cases may not be as deep.

The level of interest in this technology from current and prospective clients as well as investors is manifest in the number of acquisitions the machine learning platform market has seen in recent years, as illustrated in Table A. ThreatMetrix is a bit of an outlier—while it offers a machine

2. "Breach Level Index," Gemalto, accessed March 16, 2019, http://breachlevelindex.com.

3. See Aite Group's report *Machine Learning for Fraud Mitigation: The Substance Behind the Buzz*, April 2017.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

learning platform, its core offerings lie in its digital identity verification service, which was the primary driver for its acquisition by LexisNexis Risk Solutions. The acquisitions thus far are likely not the last, and the multiples will continue to be high given the market's rapid pace of growth.

Table A: Recent Machine Learning Platform Acquisitions

Acquired firm	Acquiring firm	Announcement date	Purchase price (In US$)
Alaric	NCR	December 2013	$84 million
Brighterion	Mastercard	July 2017	Undisclosed
Intellinx	Bottomline Technologies	January 2015	$67 million
Simility	PayPal	June 2018	$120 million
ThreatMetrix	LexisNexis Risk Solutions	January 2018	$817 million

Source: Aite Group

MACHINE LEARNING FOR AML USE CASES

While fraud use cases have led the way in terms of adoption of machine learning platforms and models, the AML environment is gaining momentum as well. Concern over regulators' requirement for fully transparent and explainable analytics has long been an obstacle to widespread adoption of advanced analytics in AML, but the tide is slowly shifting. An important signal came from U.S. regulators in December 2018, when the U.S. Treasury Department's AML unit and the federal banking regulators issued a joint statement to encourage FIs to consider innovative approaches to AML. One of the global acquiring processors interviewed for this report has had machine learning in production for a couple of years for AML transaction monitoring and sanction screening use cases, and the interviewee says that the firm has weathered regulatory exams in multiple countries without an issue. In fact, this executive says that the firm's Dutch regulator has commended its analytic approach to AML compliance. Another FI interviewed for this report has unsupervised AML transaction monitoring models in production in Singapore, with the full cooperation and approval of its regulator.

Wheels of progress do not always spin rapidly when banking intersects regulation, however, and the use of machine learning for AML use cases is still in early stages. One of the large European banks interviewed has unsupervised machine learning in proof of concept (POC) but has not yet shared the concept with its regulator—this bank plans to wait another six months until sufficient results have been compiled in the hopes of sharing results so compelling that it convinces the regulator that the machine learning approach is superior to its legacy rules-based system. The good news for the industry is that the tipping point may be rapidly approaching for a more widespread embrace of advanced analytics for AML.

THE INCUMBENTS' AND THE NEWCOMERS' CHALLENGES

Long-time incumbents in most markets bring innate advantages, in the form of established client relationships, in-depth understanding of use cases, and an established place within the IT stack.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

These vendors typically know how to navigate banks' onerous vendor risk management processes (and have already done so at many FIs). The fraud and AML platform market is no different.

However, large incumbents have their challenges as well (as banks know all too well, in the face of fintech challengers that seek to chip away at their long-established revenue streams). Large incumbent firms are often less nimble than startup challengers, given the need to dedicate resources to product maintenance and service for their established client base at the same time they are trying to innovate. As the enterprise fraud and AML detection platform market is evolving from its initial incarnation, which relied heavily on relational databases and rules, to the next generation of technology, this challenge is particularly exacerbated for its incumbents. Clients' IT organizations' ability to consume and deploy new versions of legacy systems has been hampered by lack of resources and competing budget priorities. As a result, deploying the latest and greatest production versions tends to lag, and, in some instances, clients opt for a new procurement cycle through a request-or-proposal (RFP) process versus investing in upgrades to incumbent technology.

The install base for legacy vendors is largely on relational databases with rigid data models. The process of decoupling the rigid data model and moving to a big-data structure is a significant challenge. Most incumbent vendors have accomplished this by developing add-on services that can build advanced machine learning models in a separate environment and import them into the core platform, and all are working on strategies to migrate their services into more flexible big-data architectures, but striking the right balance between introducing competitive, leading-edge functionality and not requiring upgrades so onerous that they are the equivalent of a brand-new install (thus prompting a new procurement cycle) is not easy.

Newer vendors have the advantage of building on native big-data technology from the ground up, and because they have relatively smaller customer bases, the customer reference ratings for responsiveness and support tend to be quite high for the newcomers. A challenge that these vendors will face as they grow is how to maintain these service levels as they grow—too many vendors before them have learned this lesson the hard way, as their service and support organizations struggled to keep pace with their growth curve.

KEY MARKET TRENDS AND IMPLICATIONS

The following market trends are shaping the present and future of the machine-learning-enabling platform market (Table B).

Table B: Market Trends and Implications

Market trends	Market implications
Rising criminal attacks are fueled by rampant data breaches.	FIs and retailers are forced to absorb more fraud losses or insert friction, which adversely impacts the customer experience.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

Market trends	Market implications
Regulators are encouraging FIs to use more sophisticated detection techniques.[4]	Especially in the AML space, concern over regulatory response to the use of machine learning has been an inhibitor to adoption. The new openness among regulators will further fuel market growth.
Technology advances have enabled faster and more predictive analytics.	More scalable processing, big-data technologies, reduced data storage costs, and a democratization of data sciences have enabled significant advancement in analytical capabilities over the past decade.

Source: Aite Group

4. Penny Crosman, "Is Regulators' Green Light on AML Tech a Game Changer?" American Banker, December 5, 2018, accessed January 2, 2019, https://www.americanbanker.com/news/is-regulators-green-light-on-aml-tech-a-game-changer.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

KEY PURCHASING DRIVERS

While many reasons lead to purchasing, the following represent the key factors:

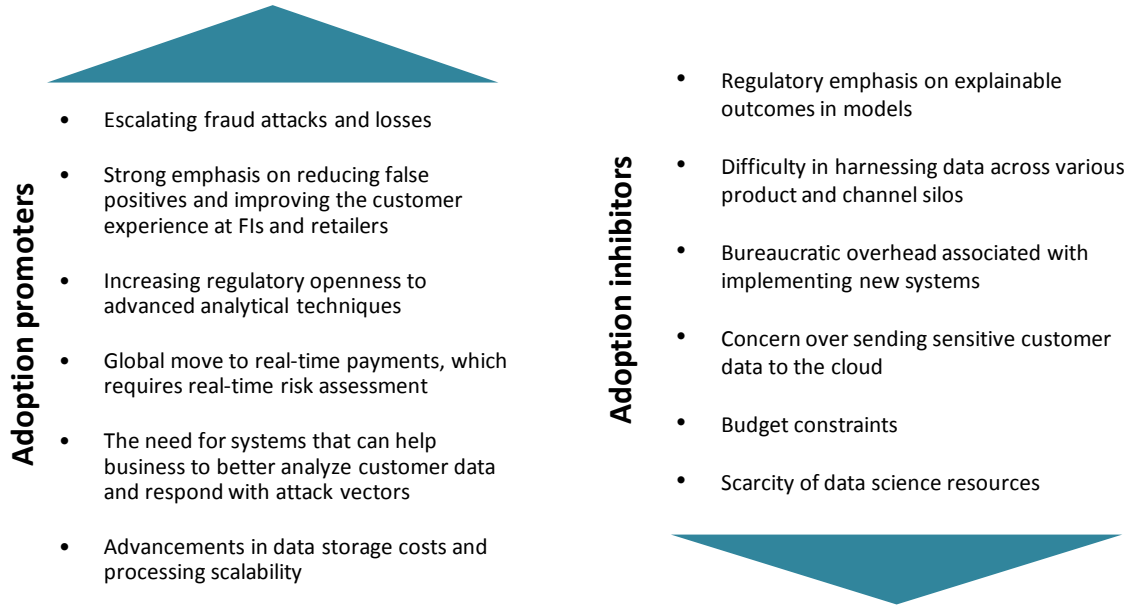
- **Business need:** Mounting fraud losses or an AML system that is unable to deal with rising transactional volume while meeting regulatory expectations is usually a key driver behind the need to find a new detection engine. Customer impact is also a key driver. One FI interviewed for this report has a top-down mandate for a new card fraud detection engine, after C-level executives and their acquaintances received repeated false declines at the point of sale on their debit card transactions.
- **Performance**: As firms are looking for a new detection platform, the detection rate and false-positive rate are among key metrics that will determine a solution's performance.
- **Service and support**: Regardless of how effective a solution's performance is, responsive service and support are essential to maintaining a positive client relationship. As firms are looking for new solution providers, service responsiveness is a key criterion for executives interviewed.
- **Cost**: Total cost of ownership is an inevitable component of any business case, although for most of the firms interviewed, superior performance and service levels take priority over cost considerations.

KEY DRIVERS FOR AND AGAINST ADOPTION

Figure 5 provides an overview of the key factors contributing to overall adoption as well as the challenges for vendors to penetrate additional prospects. The ensuing discussion elaborates upon each of these points.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

Figure 5: Factors for and Against Adoption



Source: Aite Group

Drivers for adoption include the following:

- **Escalating fraud attacks and losses**: Account takeover (ATO), card-not-present (CNP) fraud, and application fraud are on the rise for firms across the globe, driving the need for better and more nimble financial crime detection engines.
- **Emphasis on reducing false positives**: Consumers' expectations are increasingly shaped by the friction-free experiences provided by Apple, Lyft, Amazon, etc. False declines often lead to customer attrition, so FI and retail executives are under heavy pressure to reduce this impact.
- **Increasing regulatory openness to advanced analytical techniques**: Regulators have signaled increasing openness to advanced analytics in public statements. One vendor interviewed for this report has an AML detection pilot underway using machine learning analytics, in which the Financial Crimes Enforcement Network (FinCEN) has given the participating FI full exemptive relief. This signals a sea change in regulators' view of advanced analytics.
- **Global move to faster payments**: Over 40 countries have enabled a faster payments scheme, with more on the way. Faster payments mean faster fraud, and FIs are looking for systems with real-time detection and interdiction capabilities to help them manage the risk.
- **The need to better analyze customer data**: In the face of the rising threat landscape, a key asset that FIs, processors, and retailers can use to combat the risk is their customer data. Harnessing the power of that data and turning it into intelligence is a key challenge, however, that requires next-generation financial crime analytical engines.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

- **Advancements in underlying technologies**: The cost to store data has reduced dramatically over the past 20 years; as a result, more data is available to inform advanced analytics. At the same time, processing speeds have increased, enabling the analytics to process the data more quickly.

Drivers against adoption include the following:

- **Regulatory emphasis on explainable outcomes**: While regulators are displaying a new openness toward advanced analytics, there is still a heavy emphasis on model transparency and explainable outcomes for both fraud and AML models. This can be an inhibitor to adoption, particularly in the case of unsupervised models.
- **Difficulty in harnessing data**: In Aite Group's Q4 2017 survey of FIs on their use of machine learning analytics for fraud mitigation, the challenge of harnessing and cleansing FIs' own internal data was cited as one of the biggest challenges.
- **Bureaucratic overhead**: Bureaucratic overhead within firms, especially FIs, is a key hurdle to adoption. Business cases need to be justified, IT resources need to be corralled, and in the case of FIs, vendor risk management processes must be navigated. FIs interviewed for this report say that this process can take 18 to 24 months to navigate, which is an eternity in the face of rapidly evolving and escalating fraud and money laundering attacks.
- **Data security concerns**: While cloud-based implementations can not only help shortcut some of the front-end implementation time frame but also drastically improve ongoing maintenance costs and timely access to the latest and greatest platform functionality, many FIs still are reticent to send sensitive client data to the public cloud. This tide is beginning to turn, however. Two large European FIs interviewed for this report are in the process of deploying public-cloud fraud and AML detection across multiple use cases, citing the expense efficiencies and the benefits of having immediate access to vendor enhancements without the cumbersome on-premises upgrade process.
- **Budget constraints**: Budget is always an issue, and these machine learning platforms are not cheap. A large regional FI interviewed for this report will have to spend nearly US$1 million to deploy a fraud-enabling platform for just one use case, so cost is certainly a big consideration.
- **Scarcity of data science resources**: While most vendors offer professional services resources to help with model creation and maintenance, many of the FIs interviewed want to have ownership and oversight. Unfortunately, skilled data science resources are difficult to come by and, in some geographic markets, even harder to retain.

MACHINE LEARNING MODEL DEVELOPMENT PROCESS

The primary goal of firms investing in machine learning platforms is to improve their ability to detect fraud or money laundering while reducing false positives, and to have analytics that can

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

nimbly and responsively evolve with emerging attack vectors. To reach this goal, a good deal of prep work must happen first. The following outlines at a high-level the typical model development process. Best-in-class machine learning platforms will have a native ability to support these steps:

- **Data ingestion and cleansing:** A model is only as good as its inputs, and firms must first corral and cleanse the various internal and external data inputs. This is often one of the most time-consuming aspects of a machine learning platform deployment. One large bank executive says it took his FI almost a year to get the requisite info from its core banking platform and other internal sources and cleanse it. Another executive says that for any new modeling effort, his team typically spends 80% of its time on data wrangling and 20% on the actual modeling effort.
- **Data exploration and feature generation:** This stage entails an examination of the raw data and extraction of predictive features that can drive the modeling. This process can take weeks, although some of the leading platforms provide automation of the feature generation process that can accomplish this step in hours.
- **Model development and comparison:** Once the features are identified, the model development process begins. While this can include manual involvement by data scientists who iterate on the versions until the optimal results are isolated, many leading platforms provide some degree of automation for this function. This can include developing multiple models with different algorithms and providing a comparison of the various models' performance. BAE Systems' platform provides a good graphical depiction of this in the form of a heat map (Figure 6).
- **Testing:** Once the optimal model is developed, it will be tested against historical data sets in a sandbox to determine the model's impact on detection as well as the expected volume of alerts.
- **Deployment:** When ready, the model will be deployed into production. Most FIs require the platform to enforce a workflow that demands multiple approvals before a model can be deployed.

Figure 6: Model Performance Comparison

ID	Experiment	Dataset	Featureset	Algorithm [Engine]	Validation	ROC	Accuracy	TP%	FP%	FP : TP	F1	F2	F0.5	▼AUC	Actions
39	Payment Experiment	May-Aug 2014 - [Class 1.0 (10%)]	info100	AdaBoost [Smile]	cross-5		94.2%	61.1%	2.1%	0.316	67.7%	63.6%	72.5%	0.957	Apply
222	Payment Experiment	May-Aug 2014 - [Class 1.0 (10%)]	info100	Neural Networks [Smile]	split-0.2		93.4%	57.3%	2.3%	0.325	65.1%	60.2%	71%	0.929	Apply
40	Payment Experiment	May-Aug 2014 - [Class 1.0 (10%)]	info100	Gradient Boosted Trees [Smile]	cross-5		93.9%	50.2%	1.2%	0.221	62.3%	54.4%	72.7%	0.916	Apply
41	Payment Experiment	May-Aug 2014 - [Class 1.0 (10%)]	info100	Neural Networks [Smile]	cross-5		92.7%	54.4%	3%	0.496	60%	56.5%	63.9%	0.897	Apply
195	Payment Experiment	May-Aug 2014 - [Class 1.0 (10%)]	info100	Neural Networks [Smile]	cross-5		92.3%	59.1%	4%	0.609	60.6%	59.7%	61.5%	0.893	Apply
38	Payment Experiment	May-Aug 2014 - [Class 1.0 (10%)]	info100	Probability(Naive Bayes) [Core]	cross-5		86.1%	71.4%	12.2%	1.54	50.7%	61.4%	43.3%	0.868	Apply
37	Payment Experiment	May-Aug 2014 - [Class 1.0 (10%)]	info100	Logistic Regression [Core]	cross-5		92.5%	36.6%	1.3%	0.318	49.4%	40.9%	62.5%	0.848	Apply
42	Payment Experiment	May-Aug 2014 - [Class 1.0 (10%)]	info100	Random Forest [Smile]	cross-5		93.4%	42.2%	0.9%	0.194	56.1%	46.8%	69.9%	0.842	Apply
36	Payment Experiment	May-Aug 2014 - [Class 1.0 (10%)]	info100	Rule Induction [Core]	cross-5		93.4%	57.9%	2.6%	0.41	63.8%	60.1%	67.9%	0.783	Apply

Source: BAE Systems

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

KEY FUNCTIONALITY

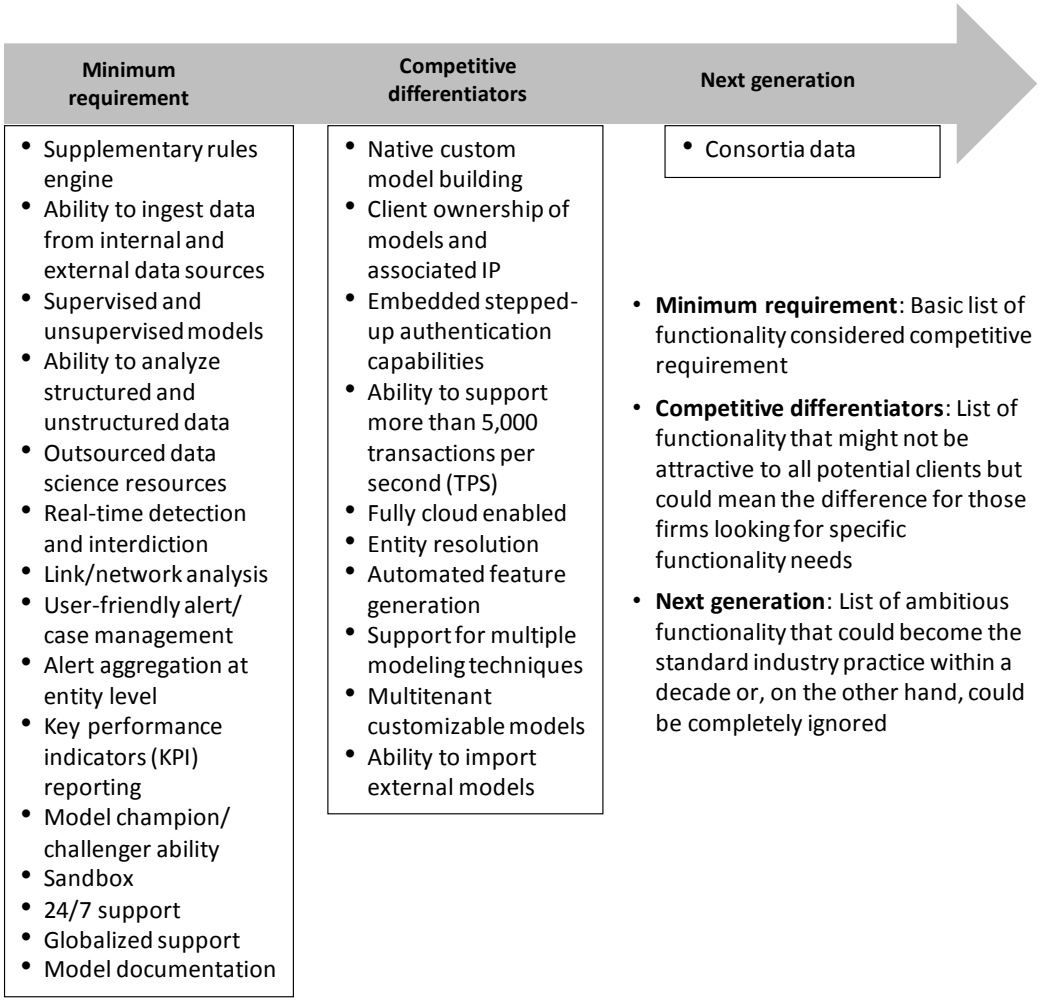
When it comes to key functionality, a set of minimum requirements must be met in order to sustain the basic needs of the clients. These minimum requirements are typically the same across regions and are found in nearly all vendors in the market.

In order to increase overall adoption and capture additional market share, vendors are focused on developing functionality that presents competitive differentiators. Competitive differentiators might not be attractive to all potential clients, but they are driving key client adoption and often could mean the difference for those firms looking for specific functionality needs. Features noted as next-generation could become the standard industry practice within a few years; on the other hand, they could be completely ignored. Given the limited resources within each vendor, it is imperative that appropriate investments are made across the needs of past, current, and future clients.

In the machine learning space, an added challenge when prioritizing product development is the widely varying needs of the customer base. Large global FIs and merchants often have robust internal data science teams that want to deploy their own internally developed models. Regional banks typically want to rely on the platform's model development capabilities and often the vendor's outsourced data science resources for custom model development. Processors are often looking for multitenant capabilities that enable the processor to customize the models across its diverse client base. While a good chunk of the platform requirements overlap for these target markets, a fair amount of required functionality is unique to each. The minimum requirements, competitive differentiators, and next-generation attributes are briefly described in Figure 7.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

Figure 7: Key Functionality Trend



Source: Aite Group

MINIMUM REQUIREMENTS

- **Supplementary rules engine:** While advanced analytics are critical to increasing detection rates and reducing false positives, the ability to strategically insert rules is also deemed essential by the majority of fraud and AML executives.[5]

- **Ability to ingest and analyze data from internal and external sources:** Harnessing internal data sources from multiple product silos and channels is often one of the most challenging parts of platform implementations, but it is a baseline requirement, as is the ability to enrich internal data with external feeds, such as digital identity verification, public record data, and/or consortium data.

- **Ability to ingest structured and unstructured data:** While many firms are just beginning to tap into unstructured data sources, these can provide a robust set of

5. See Aite Group's report *Machine Learning: Fraud Is Now a Competitive Issue*, October 2017.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

inputs to analytical models for both fraud and AML. The ability to ingest and analyze these data sources is an important attribute to look for in a vendor solution.

- **Support for supervised and unsupervised models:** Supervised models are created using labeled training data, i.e., data that has been specifically identified as either a bad or good transaction. This approach is ideal to use when a good amount of historical data is available to train the analytics. Unsupervised models do not rely on labeled training data and are useful when the organization doesn't have a lot of history to use for modeling (e.g., with new payment methods, such as faster payments, or in AML). The answers are not known in advance, so the system is learning to detect outliers based on their similarity to prior transactions. Unsupervised models can still be challenging to deploy in the highly regulated banking environment, with its heavy emphasis on model governance, since clearly explaining the causality in these models can be difficult.

- **Real-time detection and interdiction:** As faster payment methods expand across the globe, the ability for platforms to ingest streaming data and provide real-time decisioning and interdiction is critical for effective risk management.

- **User-friendly alert and case management:** Analysts and investigators spend the majority of their days interacting with their vendors' alert and case management interfaces. There is a lot of science and a little bit of art in designing these interfaces to present the most useful information possible in the most user-friendly manner. A good user interface (UI) can reduce the number of clicks and shave minutes off each alert or case worked, which has a big impact on KPIs.

- **KPI reporting:** To measure the effectiveness of a solution, as well as emerging fraud trends, good KPI reporting is essential, in the form of customizable and configurable management dashboards.

- **Model champion/challenger ability:** As new models are developed, it's important to have the ability to test them to determine whether they will deliver improved results. Many systems enable this capability.

- **Sandbox:** Before deploying new models, it's essential that a business can test new models to understand their impact on alert workloads. A sandbox environment enables this by testing new analytics on historical data without impacting production workload.

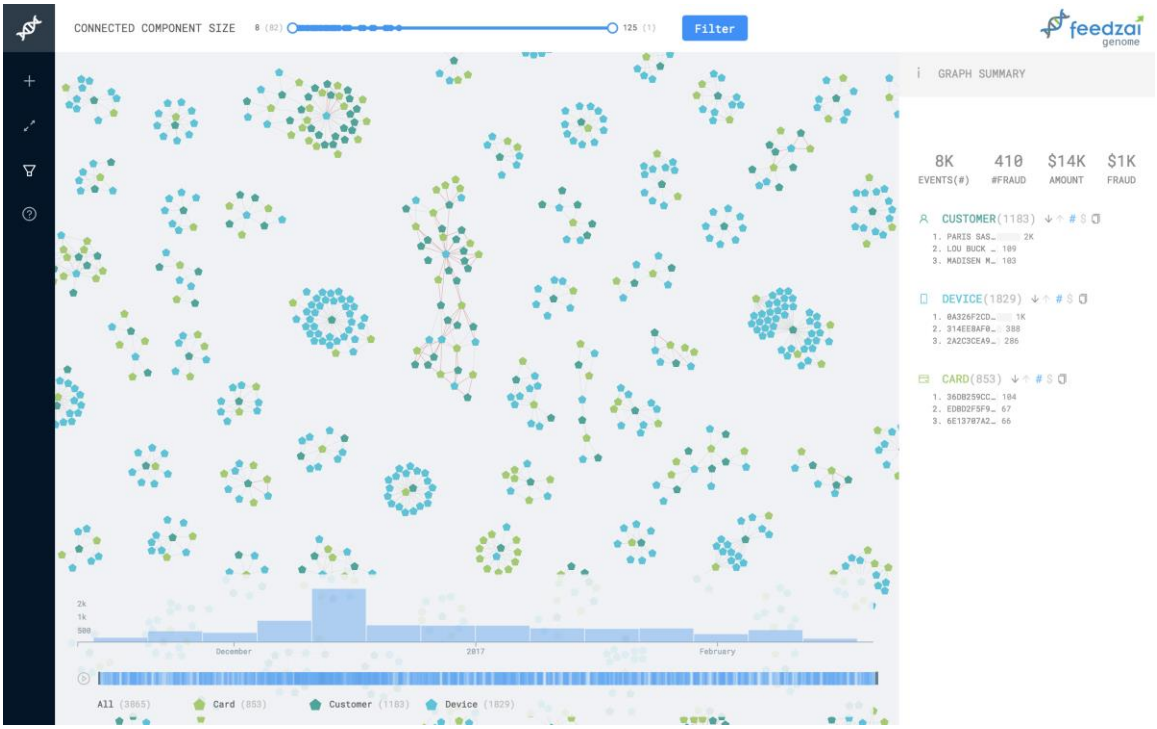
- **24/7 and globalized support:** Financial crime does not adhere to business hours or geographies, and vendor solutions need to be able to support the always-on, global nature of the business.

- **Model documentation:** Regulators want to know that banks have a clear understanding of how their models work, how any changes impact detection and false positives, and whether the use of vulnerable variables leads to prejudicial outcomes. To that end, regulators as well as internal model governance teams require extensive documentation of how models function and the impact of any changes made to the models.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

- **Link/network analysis:** Link analysis tools sift through the data repositories and discover connections between customers and accounts, then graphically display them to facilitate investigation. Some connections are innocuous; others are highly suspicious. When properly applied, link analysis and data visualization are useful for both detection and investigations. The ability to refresh networks frequently is important given the pace of financial crime—refresh frequency is a key question that should be asked when evaluating firms' capabilities on this front, since many firms cannot support intraday refreshes due to the heavy data load. Figure 8 provides a good example of graphical link analysis.

Figure 8: Example of Link Analysis



Source: Feedzai

COMPETITIVE DIFFERENTIATORS

- **Native custom model building:** The ability to enable businesses to build and deploy custom machine learning models across a variety of fraud and AML use cases is a key reason why many firms are actively looking for new vendor partners. Attack vectors evolve rapidly, and the legacy approach that relies heavily on rules or analytical models that are only refreshed every year or two is no longer sufficient.

- **Client ownership of models and associated IP:** While many firms will lean on their vendor partner initially for model development, many of those interviewed want to have ownership of the IP and the ability to eventually dedicate their own data science resources to model refreshes.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

- **Embedded stepped-up authentication capabilities:** While detection of a fraud event is important, a key requirement for many of the firms interviewed for this report is that the platform provide an embedded ability to interact with the customer via two-way text, mobile app push, or email in order to help resolve the alert in real time.

- **Ability to support more than 5,000 TPS:** From real-time payments to payment cards, machine learning platforms have to be able to process a significant load of real-time transactions with subsecond response times, though TPS will vary based on the data load. While the tolerance for latency is a greater for most AML use cases today, many AML processes are increasingly moving in the direction of real-time as well.

- **Cloud enabled:** Cloud-based deployments are attractive for their scalability and expense-reduction potential, and they enable firms to access the latest and greatest version of vendors' solutions without onerous IT projects. While FIs in particular have been relatively slow in embracing the cloud for fraud and AML solutions, that sentiment is shifting. Two large European FIs interviewed for this report are in the process of moving substantial portions of their financial crime detection to the public cloud, while a midsize U.S. regional bank is going to market with an RFP that includes cloud deployment as a requirement.

- **Entity resolution:** With multiple internal and external data sets with disparate schemas and levels of quality feeding the analytics, the ability to dedupe and resolve the inputs or alerts into a single customer view is important to managing the alert volume and output quality.

- **Automated feature generation:** The data wrangling that goes into model building is quite time-consuming. After acquiring the data and cleansing it, there is often a lengthy feature generation process in which data scientists determine the optimal set of features to drive the models. Some of the enabling platforms offer automated feature generation, in which the platform generates the features, builds multiple models, and provides comparisons of model and feature performance.

- **Support for multiple modeling techniques:** A variety of modeling techniques falls under the machine learning umbrella—random forests, neural networks, XGBoost, and logistic regression, just to name a few. Depending on the type of fraud or money laundering scheme, some modeling techniques work better than others, so best-in-class platforms will enable a range of modeling techniques.

- **Multitenant customizable models:** Processors need a multitenant capability that enables them to push a variety of customizable models to their issuer or merchant clients. Some issuers have contactless cards in market, and some do not. Some issuers are working toward 3-D Secure 2.0 enablement, which provides a wealth of incremental data to inform CNP decisioning, and others will lag. It is important for processors to be able to ingest the data their clients can provide and optimize models for their clients' capability set.

- **Ability to import external models:** Large banks and merchants often have substantial internal data science teams that prefer to build their own models in R,

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

Python, etc. Best-in-class platforms will support this need and facilitate easy upload using standard methods such as Predictive Model Markup Language (PMML).

NEXT-GENERATION CAPABILITIES

- **Consortia data:** Shared intelligence can provide an enormous amount of value to financial crime mitigation solutions, since crime rings will attack multiple points of the financial value chain simultaneously. With increasing levels of regulation around data privacy, the mechanism to facilitate antifraud consortia is not easy, however, so this is still an emergent capability in the enabling platform space.

THE ROLE OF CONSULTANTS

Many FIs engage consultants on an ongoing basis to help with systems integration, performance optimization, and regulatory audit services. While a number of the vendors have professional services functions that can assist on this front, many FIs choose to use external consultants. The consultant firms also serve as a valuable sales channel for the vendors, since they will often recommend a vendor when the consultancy has been engaged to analyze and recommend improvements to legacy financial crime processes. Table C lists the consultancy and systems integration partnerships in place for the vendors participating in this report.

Table C: Consultancy and Systems Integration Partnerships

Firm	Consultant/systems integrator partner(s)
Brighterion	Unisys
DataVisor	Accenture, PwC
Featurespace	everis, Icon Solutions, PwC
Feedzai	Deloitte
Nice Actimize	PwC, Matrix, Unisys, AGS Nasoft, Deloitte, DIS-Group, Infosys, IBM Japan, Q2 Technologies, Stream IT
SAS	Ernst & Young, Accenture, Capco
Simility	Finacle, HCL
ThetaRay	PwC

Source: Vendors

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

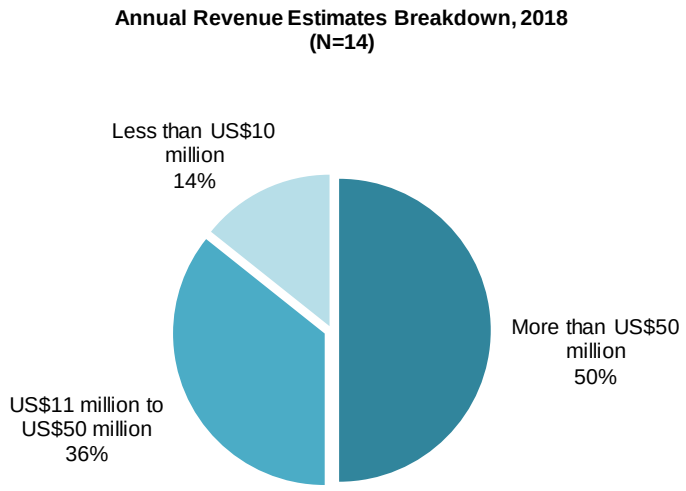
KEY STATISTICS AND PROJECTED IT SPENDING

This section provides information and analysis on key market statistics as well as projected IT spending related to the vendor market.

ANNUAL REVENUE ESTIMATES ANALYSIS

The vendors that provide machine-learning-enabling platforms consist of both long-time market incumbents—such as FICO, SAS, Nice Actimize, and BAE Systems—and new entrants—such as Feedzai, Featurespace, ThetaRay, Simility, and DataVisor. Half of the vendors earn more than US$50 million in revenue per year, with giants such as SAS, ACI Worldwide, and FICO earning considerably more (Figure 9).

Figure 9: Annual Revenue Estimates Breakdown



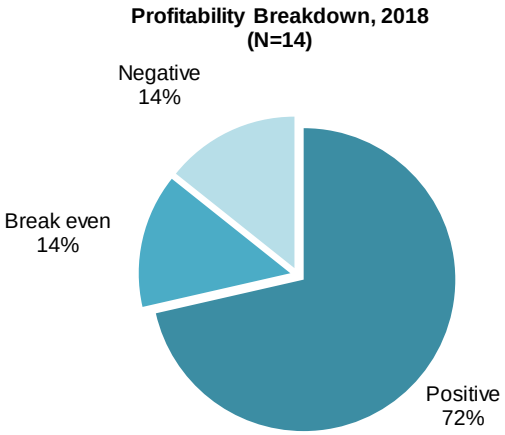
Source: Vendors

PROFITABILITY ANALYSIS

While half of the participating vendors are relatively new to the market, having been founded in 2005 or later, the majority of participating vendors either are profitable or break even, which speaks to the rapidly expanding nature of the space (Figure 10).

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

Figure 10: Vendor Profitability

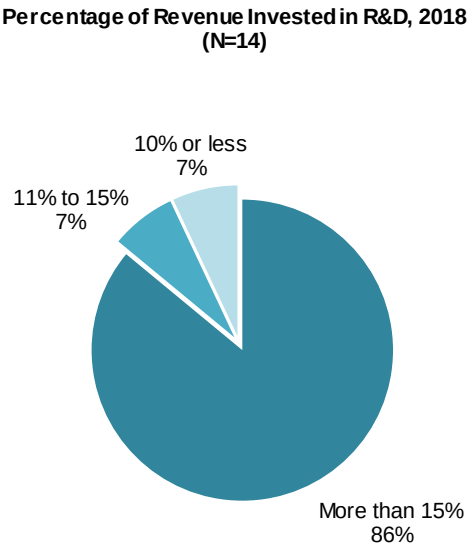


Source: Vendors

R&D INVESTMENT ANALYSIS

The rapid pace with which crime is growing and evolving dictates equally rapid development on the part of vendors that enable the compensating controls. The vast majority of vendors in the space invest more than 15% of their revenue in ongoing R&D (Figure 11). The vendors that fall into the 15% or less category are larger vendors that have higher levels of annual revenue, thus making it harder to hit the higher percentages of revenue invested in R&D, given the larger denominator.

Figure 11: Percentage of Revenue Invested in R&D



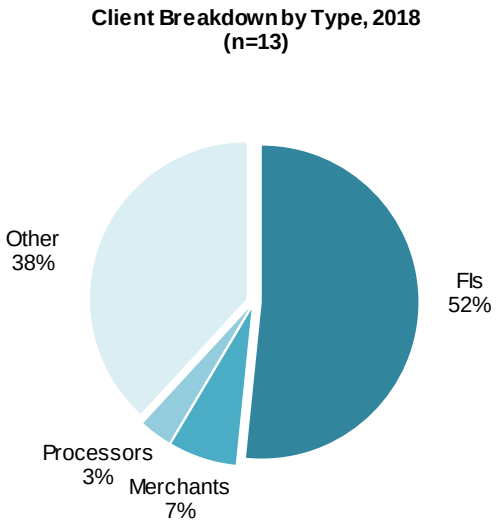
Source: Vendors

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

CLIENT BREAKDOWN BY TYPE

FIs represent the bulk of the client base for participating vendors, which stands to reason—FIs are large in number, they are intensely targeted by fraud and money laundering, and they have the budget to support the expense associated with these platforms. While merchants as a target segment are also numerous, only a small subset of the merchant target market can afford the expense associated with machine learning platforms. Processors represent 3% of the client install base—while they both have the need and the budget to support the expense, there are far fewer processors across the globe than there are FIs. Bottomline Technologies represents a solid portion of the "other" category, given its large corporate customer base (Figure 12).

Figure 12: Client Breakdown by Type



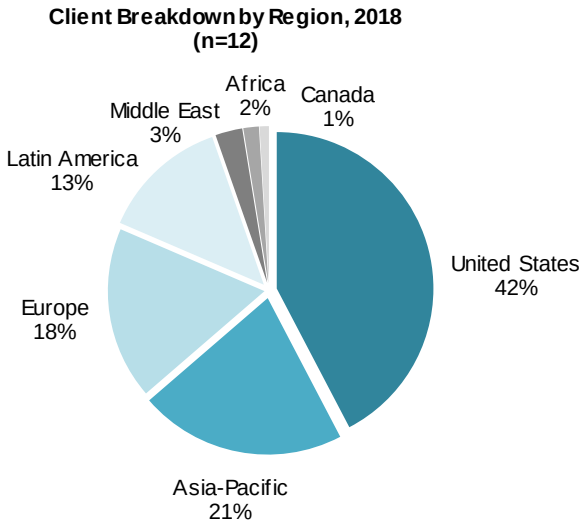
Source: Vendors

CLIENT BREAKDOWN BY REGION

The client breakdown among participating vendors spans a wide geographical range. The U.S. represents 42% of the client installs, but the Asia-Pacific and Europe are also well-represented (Figure 13).

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

Figure 13: Client Breakdown by Region

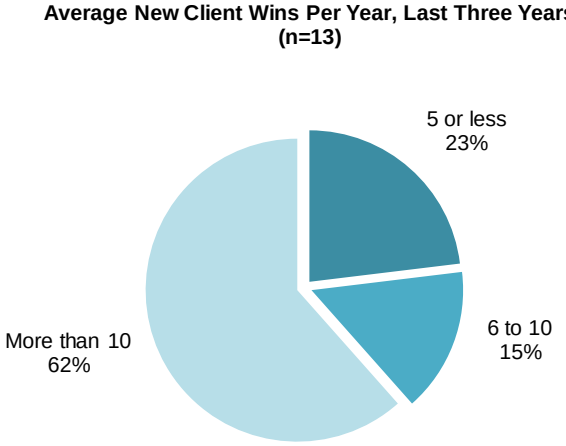


Source: Vendors

AVERAGE NEW CLIENT WINS

The amount of investment pouring into this space is evident in the average number of annual client wins reported by the vendors over the past three years. More than half of the vendors are winning more than 10 new clients per year (Figure 14).

Figure 14: Average New Client Wins in the Last Three Years



Source: Vendors

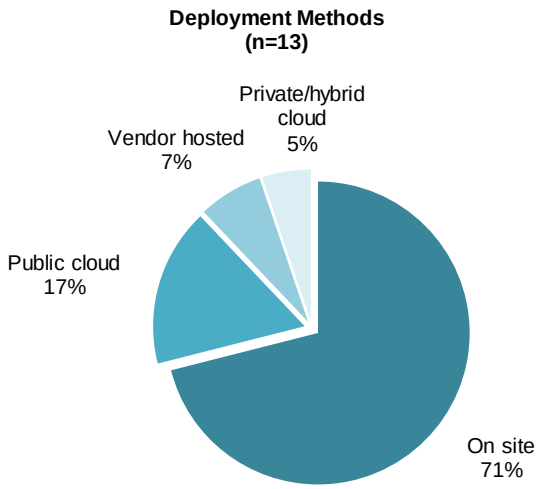
101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

DEPLOYMENT ANALYSIS

Financial crimes units have lagged other areas of FIs in terms of embracing cloud-based deployments, due to concerns over data security, latency, and customization capabilities. The proportion of cloud to on-premises deployments bears out the trend to date (Figure 15). In the interest of consistency of definitions, a vendor's deployment with a processor or network such as TSYS, FIS, or Mastercard counts as one on-premises deployment (Figure 15 does not individually count the many FIs that consume risk scores from that vendor via a call to the processor).

While the majority of deployments of machine-learning-enabling platforms are still on-premises, a number of the interviews conducted for this report indicate that the market may be gradually making its way toward a tipping point. Two Tier-1 European FIs interviewed are in the process of migrating substantial portions of their financial crime detection to the public cloud (one with AWS, the other with Azure). Another midsize U.S. FI is in the process of deploying an RFP for a machine-learning-enabling platform, and cloud enablement is a baseline requirement. The ability to access the latest and greatest platform functionality without onerous IT upgrades, cost, and scalability is a key consideration that tips the business case in favor of cloud for these FIs.

Figure 15: Deployment Options



Source: Vendors

The path to the cloud is not without its bumps. The large European bank that is deploying on Azure says that this is one of the earlier public-cloud implementations for the bank, so there is a big learning curve. The fraud team and its vendor have to spend quite a bit of time with the bank's data security folks as well as regulators to establish a comfort level and ensure the requisite controls are in place. The Tier-1 European bank is using a vendor's AWS-deployed platform and says that its internal data security team had an incremental 240 data security controls that the vendor had to put in place before it would give its blessing for sensitive customer data to be sent to the public cloud.

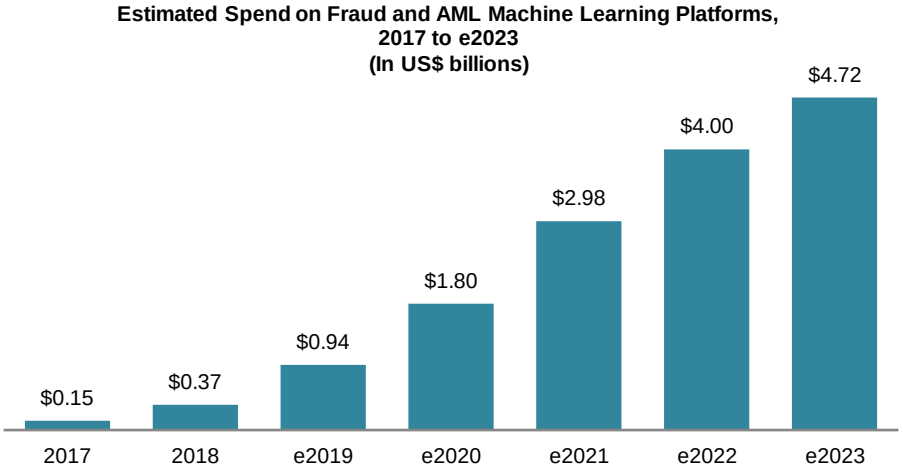
101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

PROJECTED SPENDING

Aite Group's spending estimates on the financial-crime-enabling market include the software license, integration, and maintenance fees. This spending estimate also includes the professional service fees associated with data integration, model building, and maintenance.

Global spending on financial-crime-enabling platforms will be almost US$1 billion by the end of 2019 and is expected to reach US$4.72 billion by the end of 2023 (Figure 16).

Figure 16: Projected Global Spending on Financial Crime Machine Learning Platforms



Source: Aite Group

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

VENDOR COMPARISONS

This section presents comparative data and profiles for the individual vendors that participated in the AIM evaluation. This is by no means an exhaustive list of vendors, and firms looking to undergo a vendor-selection process should conduct initial due diligence prior to assembling a list of vendors appropriate for their own unique needs. Table D presents basic vendor information for the participating solutions, and Table E provides high-level product information.

Table D: Basic Vendor Information

Firm	Headquarters	Founded in	Examples of clients
ACI Worldwide	Naples, Florida	1975	Westpac New Zealand
BAE Systems	London	1999	Confidential
Bottomline Technologies	Portsmouth, New Hampshire	1989	Confidential
Brighterion	San Francisco	2000	Mastercard, Morgan Stanley, Worldpay, Elavon, Safran Morpho
DataVisor	Mountain View, California	2013	Pinterest, Yelp, Ping An Insurance
Featurespace	Cambridge, U.K.	2008	TSYS, Ally Bank, Worldpay, Danske, Vocalink
Feedzai	San Mateo, California	2009	Citibank, Lloyds, First Data, Leumi Card
FICO	San Jose, California	1956	FIS, UBS Card Center, EnterCard, Network International
Nice Actimize	Hoboken, New Jersey	1999	Confidential
Risk Ident	Hamburg, Germany	2012	Otto Group, Deutsche Telekom, Vodafone
SAS	Cary, North Carolina	1976	Confidential
Simility	Palo Alto, California	2014	U.S. Bank, Chime, OfferUp, StubHub, Itau, Republic Wireless, Discover, Equifax
ThetaRay	Hod HaSharon, Israel	2013	OCBC, ABN Amro
ThreatMetrix, a LexisNexis Risk Solutions company	San Jose, California	2005	Confidential

Source: Vendors

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

Table E: High-Level Product Information

Firm	Product name(s)	Launch date	Current version	Pricing structure
ACI Worldwide	Universal Payments (UP) Proactive Risk Manager (PRM)	1997	8.8	Pricing includes license fee, maintenance, model, capacity, and implementation services.
BAE Systems	NetReveal, Advanced Analytics Platform (AAP)	2012	2.2	Standard pricing is by industry by tier; in many cases, pricing becomes a negotiated fee as a blend of software and services tailored to the customer's issue(s) in delivering a fit-for-purpose solution.
Bottomline Technologies	Cyber Fraud & Risk Management (CFRM), Secure Payments	2005	5.8	Pricing is based on the number of transactions processed per day on average.
Brighterion	Brighterion AI Platform	2003	9.0	Generally, pricing is broken into three parts: one-time enterprise license fee, support and maintenance fee, and volume-based fee.
DataVisor	DCube	2014	Software-as-a-Service (SaaS) without external version numbers	Pricing is on an annual subscription basis—depends on the use case(s), data volume, and deployment options.
Featurespace	ARIC Fraud Hub	2008	3.13	Annual license fee is based on transaction volume, plus professional services.
Feedzai	Transaction Fraud for Banks, Transaction Fraud for Acquirers and Processors, Account Opening, Anti-Money Laundering, Transaction Fraud for Merchants	2011	Pulse 19.0	Pricing is an annual license fee, plus professional services.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

Firm	Product name(s)	Launch date	Current version	Pricing structure
FICO	Falcon	1992	6.5	Tiered pricing model is based on the number of accounts monitored by portfolio type (e.g., credit, debit, retail banking).
Nice Actimize	Actimize Integrated Fraud Management (IFM) and Autonomous AML Solutions Suite	2014	4.15 (IFM-X 2019)	Solutions are licensed in packages, which are scoped by channel coverage, transaction type, number of accounts monitored, transaction volume, and region.
Risk Ident	Frida One, Frida machine learning, Device Ident	2015	1.6	Monthly license fee for SaaS is based on transactions and client user seats.
SAS	SAS Fraud Management (FM), SAS Fraud Framework (FF)	2006	6	Pricing is based on the number of active accounts per module/channel; transaction volume, real-time decisioning service level agreements (SLAs), and the number of analysts and investigators will impact the sizing and provisioning of requisite systems infrastructure.
Simility	Enterprise Fraud Management Platform (EFMP)	2016	4.5	Pricing is based on transaction volume, such as account origination, payment transactions, or logins processed through the system; it charges an additional fee for custom machine learning models, training, and data scientist or data analyst services.
ThetaRay	ThetaRay analytics platform	2015	3.4.1	Value-based pricing is on a subscription basis. Standard pricing structure includes annual subscription fees for the following components: ThetaRay analytics platform, use case, and investigation center (add-on).
ThreatMetrix	ThreatMetrix Smart Analytics	2016	9.7	Pricing is transaction-based.

Source: Vendors

Table F presents high-level functional information associated with each product. TPS represents peak in production, and will vary by use case.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

Table F: Product Functional Information

Vendor	Data ingestion options	Supervised vs. unsupervised model deployments	TPS
ACI Worldwide	Data can be ingested via fixed record length, XML, web services/ application program interfaces (APIs), MQ and/or messages, and/or batch files.	100% supervised	5,000 in production, 8,000 in stress test environments
BAE Systems	Data can be brought in via drag-and-drop from a local network or via URL. AAP will interpret the data and give the option to amend.	100% supervised in production, 80% supervised and 20% unsupervised in POCs	10,000
Bottomline Technologies	The CFRM platform can be integrated with the corporate systems in several ways: noninvasive network sniffing for capturing user behavior, real-time transactions received for real-time scoring from the corporate systems through a web service or MQ, extraction from databases/data warehouse/log file/other sources, historic data received through a CSV file, and transactions received through a Representational State Transfer (REST) API.	50% supervised, 50% unsupervised	Not available
Brighterion	Natively, the system supports TCP, ISO 8583, etc., for batch and real-time scoring calls to its scoring engine. In addition, it can connect to multiple external data sources using open APIs or through standard database connections (ODBC, JDBC, etc.).	50% supervised, 25% unsupervised, 25% combination	62,000
DataVisor	It enables upload/download via object storage, real-time request and response via Hyper Text Transfer Protocol Secure (HTTPS) endpoint or message queue, and integration via third-party data providers.	30% supervised, 70% unsupervised	Greater than 1,000

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

Vendor	Data ingestion options	Supervised vs. unsupervised model deployments	TPS
Featurespace	Events can be submitted to ARIC in a number of ways: • HTTP: JSON formatted events are POSTed directly to a RESTful HTTP API. • Message queue: An input connector can be configured to read messages from an external message queue (e.g., Kafka, ActiveMQ, RabbitMQ, MSMQ). • Database: A database input connector can be used to extract new data from a database (SQL and NoSQL). • File: A folder can be periodically polled for new files (CSV, XML, JSON, etc.).	100% combination	16,000
Feedzai	Feedzai's solution can ingest data from RESTful API, sockets, message queues, ISO 08583, batch files, etc.	80% supervised, 30% unsupervised, with 10% of customers using both	5,000
FICO	Falcon provides both standard and user-defined APIs to integrate transaction data and events, including monetary and nonmonetary.	Credit and debit card use cases are 100% supervised models. Clients with e-payment use cases (ACH, wire, demand deposit accounts/current accounts) use 100% unsupervised models (multilayered self-calibrating models).	More than 20,000

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

Vendor	Data ingestion options	Supervised vs. unsupervised model deployments	TPS
Nice Actimize	The Actimize platform is capable of handling both flat and hierarchal input records containing any number of fields of any reasonable size and data type, whether the data is received by Actimize from a real-time source (e.g., SOAP web services or MQ messages) or queried by Actimize from batch sources (e.g., database, files). In addition, the solution can ingest raw data or alerts from other fraud, cyber, and authentication tools into a unified hub.	Actimize uses supervised models whenever the number of targets is significant enough to be able to properly train a model. For cases in which the fraud/AML event is rare, Actimize may use unsupervised machine learning models either in combination with supervised models or as an independent model.	More than 1,200
Risk Ident	It includes API, batch (CSV), and a technical integration layer and data adapter (TILDA).	80% supervised, 20% unsupervised	20 to 30
SAS	SAS Data Management is included with SAS solutions, as is a real-time intelligent middleware, which has adaptors to third-party offerings for digital and industry data. SAS Business Orchestration Services is intelligent middleware designed to support real-time/millisecond requests and response event/message processing. It's integrated with the SAS Fraud Management solution and is able to send any message type, in any format, from new and existing systems. This component acts as middleware to facilitate interactions between systems and processes.	50% supervised, 50% unsupervised	More than 10,000
Simility	Data integration can be done using REST, MQ, or Kafka and can process formats such as MQMFT, JSON, XML, HTML, CSV, and TXT. Data can be processed in streaming or batch mode.	70% supervised, 20% unsupervised, 10% semisupervised	5,000

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

Vendor	Data ingestion options	Supervised vs. unsupervised model deployments	TPS
ThetaRay	Data is generally fed into ThetaRay via JSON over REST API. Batch files may also be also be provided via database or flat file feeds.	Majority unsupervised, some semisupervised	70
ThreatMetrix	ThreatMetrix is both a producer and consumer of data. All device and network-level information from the core ThreatMetrix solutions are fed into the models. From an integration point of view, ThreatMetrix supports both "push and pull." • Push: ThreatMetrix accepts data into its API designed for e-commerce, banking, and other use cases around new account origination, login, account management, and payments. It includes input fields for account and personally identifiable information, event context, and segmentation context. In addition, it supports over 50 customer-defined fields, e.g., consuming other systems' scores. • Pull: ThreatMetrix integration hub allows for pulling data from API end points in real time. This can be any real-time API that exposes an HTTP-based protocol. Data coming back from such integrations can be embedded in models, rules, and other constructs. In addition to those, ThreatMetrix can accept truth data (labels) from various sources.	Custom model deployments are largely supervised.	12,000

Source: Vendors

Table G presents each vendor's standard client service offerings. For certain vendors, stronger client support will be available with an additional fee.

Table G: Client Service Support

Vendor	SLA	Online issue tracking	Single point of contact*	24/7 support*	Global/ localized support*	On-site training*	Online training*
ACI Worldwide	■	■	■	■	■	■	■

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

Vendor	SLA	Online issue tracking	Single point of contact*	24/7 support*	Global/ localized support*	On-site training*	Online training*
BAE Systems	■	■	□	■	■	■	■
Bottomline Technologies	■	■	■	■	■	■	■
Brighterion	■	■	■	■	■	■	■
DataVisor	■	■	■	■	■	■	■
Featurespace	■	■	■	■	■	■	■
Feedzai	■	■	■	■	■	■	■
FICO	■	■	■	■	■	■	■
Nice Actimize	■	■	■	■	■	■	■
Risk Ident	■	□	■	■	■	■	■
SAS	■	■	■	■	■	■	■
Simility	■	■	■	■	■	■	■
ThetaRay	■	■	■	■	■	■	■
ThreatMetrix	■	■	■	■	■	■	■

Source: Vendors
Key: ■= Yes; □= No
** = Standard service with no additional fee*

Table H presents each vendor's ability to support various deployment options.

Table H: Product Deployment Options

Vendor/product(s)	On site	Vendor hosted	Public cloud	Private/hybrid cloud
ACI Worldwide/ PRM	■	■	■	■
BAE Systems/NetReveal, AAP	■	□	□	■
Bottomline Technologies	■	■	■	■

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

Vendor/product(s)	On site	Vendor hosted	Public cloud	Private/hybrid cloud
Brighterion/ Brighterion AI Platform	■	■	◪	■
DataVisor/ DCube	■	□	■	■
Featurespace/ARIC	■	□	■	■
Feedzai/Feedzai	■	□	■	■
FICO/Falcon	■	■	■	■
Nice Actimize/IFM	■	■	■	■
Risk Ident	■	■	□	■
SAS/FM, FF	■	■	■	■
Simility/EFMP	■	■	■	■
ThetaRay/ThetaRay Analytics	■	□	■	■
ThreatMetrix/Smart Analytics	□	■	□	□

Source: Vendors

Key: ■= Yes; □= No; ◪ = 2019 roadmap

Table I indicates whether the platform enables development and maintenance of models by the client, whether the vendor develops and maintains the models, and who owns the intellectual property (IP) associated with the resulting model. In most (but not all) cases, if the vendor develops the model, it owns the IP, and if the client develops the model, the client owns the IP.

Table I: Key Functionality—Model Details

Vendor	Responsibility for development		Responsibility for maintenance		Ownership of custom model IP	
	Vendor	Client	Vendor	Client	Vendor	Client
ACI Worldwide	■	■	■	■	■	■
BAE Systems	■	■	■	■	■	■
Bottomline Technologies	■	■	■	■	■	■

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

Vendor	Responsibility for development		Responsibility for maintenance		Ownership of custom model IP	
	Vendor	Client	Vendor	Client	Vendor	Client
Brighterion	■	□	■	□	□	■
DataVisor	■	■	■	■	■	■
Featurespace	■	■	■	■	□	■
Feedzai	■	■	■	■	■	■
FICO	■	■	■	■	■	■
Nice Actimize	■	■	■	■	■	■
Risk Ident	■	□	■	□	□	■
SAS	■	■	■	■	■	□
Simility	■	■	■	■	□	■
ThetaRay*	□	□	□	□	□	□
ThreatMetrix	■	■	■	■	■	■

Source: Vendors
Key: ■= Yes; □= No
**ThetaRay employs unsupervised analytics, so there are no bespoke custom models.*

Table J shows the key use cases that the vendors are actively supporting in either production or POC. The criterion for this table is that the vendor must be actively supporting the use cases either in production or POC.

Table J: Key Functionality—Support for Machine Learning Use Cases

Vendor	ACH/wire fraud	ATO	Application fraud	Check fraud	Card-present fraud	CNP fraud*	CNP fraud**	Merchant acquiring fraud	AML transaction monitoring	Sanctions screening
ACI Worldwide	■	■	■	■	■	■	■	■	□	□
BAE Systems	■	■	■	■	■	■	□	□	■	□
Bottomline Technologies	■	■	□	■	■	■	■	□	■	■

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

Vendor	ACH/wire fraud	ATO	Application fraud	Check fraud	Card-present fraud	CNP fraud*	CNP fraud**	Merchant acquiring fraud	AML transaction monitoring	Sanctions screening
Brighterion	■	■	■	■	■	■	■	■	■	■
DataVisor	■	■	■	■	□	■	■	■	■	□
Featurespace	■	■	■	■	■	■	■	■	■	□
Feedzai	■	■	■	■	■	■	■	■	■	■
FICO	■	■	■	■	■	■	□	■	■	■
NICE Actimize	■	■	■	■	■	■	■	■	■	■
Risk Ident	□	■	■	□	□	□	■	□	□	□
SAS	■	■	■	■	■	■	■	■	■	□
Simility	■	■	■	■	■	■	■	■	■	■
ThetaRay	■	■	□	□	□	□	□	■	■	□
ThreatMetrix	■	■	■	□	■	■	■	■	□	□

Source: Vendors
Key: ■= Yes; □= No
**Issuer transactional analytics*
***Merchant transactional analytics*

Table K discusses each vendor's support for some of the key competitive differentiators illustrated in Figure 7. Automated feature generation can refer to the vendor automating the feature generation process for its own model creation, or the platform surfacing an automated feature generation capability for to aid the efforts of the citizen data scientists at the client. The latter capability is less common among the platforms, though many vendors have this on their 2019 roadmap. Many of the vendors can support embedded stepped-up authentication by triggering a call in the workflow to an external vendor to serve the authentication, get the response back, and use it in the model for risk-based authentication and/or to trigger next steps. Only two vendors, ACI and FICO, offer a native customer communication service as part of the platform.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

Table K: Key Functionality—Competitive Differentiators

Vendor	Automated feature generation	Import external models	Real-time detection	Alert management aggregation at entity level	Embedded stepped-up authentica-tion	Ability to ingest and analyze unstructured data
ACI Worldwide	◪	■	■	■	■	◪
BAE Systems	□	■	■	■	■	■
Bottomline Technologies	□	◪	■	■	□	■
Brighterion	■	■	■	■	◪	■
DataVisor	■	□	■	■	□	■
Featurespace	□	■	■	■	■	■
Feedzai	■	■	■	■	■	■
FICO	◪	■	■	■	■	■
Nice Actimize	◪	■	■	■	◪	■
Risk Ident	□	■	■	■	□	■
SAS	◪	■	■	■	□	■
Simility	■	■	■	■	■	■
ThetaRay	■	□	■	■	□	■
ThreatMetrix	■*	■	■	□	■	□

Source: Source: Vendors

Key: ■= Yes; □= No; ◪ 2019 roadmap

***ThreatMetrix's automated feature generation capability is available to ThreatMetrix's professional services teams, but this capability is not available for clients to leverage via a UI for their own custom model building.*

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

AIM EVALUATION

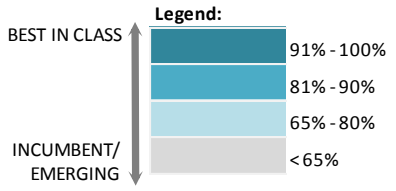
This section will break down the individual AIM components, drawing out the vendors that are strong in each area and how they are differentiated in the market. Client references are required for the AIM recognition. Risk Ident declined to provide client references, so it is not included in this portion of the analysis.

THE AIM COMPONENTS ANALYSIS

Figure 17 overviews how each vendor scores in the various areas of importance. Each vendor is rated, in part, based on its own data provided when responding to the RFI distributed by Aite Group as well as product demos and follow-up discussions as part of the AIM process. Ratings are also driven by the reference customers of the examined vendors to support a multidimensional rating.

Figure 17: AIM Components Analysis by Heat Map

Vendors	Vendor Stability	Client Strength	Client Service	Product Features
ACI	91%	73%	92%	71%
BAE Systems	80%	63%	70%	75%
Bottomline	83%	90%	78%	74%
Brighterion	88%	85%	92%	87%
DataVisor	66%	75%	90%	82%
Featurespace	88%	90%	95%	87%
Feedzai	88%	95%	85%	94%
FICO	87%	94%	84%	78%
Nice Actimize	90%	80%	79%	77%
SAS	92%	95%	79%	80%
Simility	82%	95%	90%	88%
ThetaRay	73%	89%	78%	60%
ThreatMetrix	92%	75%	85%	66%



Source: Vendors, Aite Group

VENDOR STABILITY

ACI, SAS, and ThreatMetrix scored the highest on the vendor stability front, with a number of other vendors close behind. High marks from client references for the management team, profitability, and corporate financial stability (a varied range of products contributing revenue) all contribute to strong performance in this category.

CLIENT STRENGTH

Feedzai, FICO, SAS, and Simility all scored in the best-in-class range for client strength. Key scoring drivers in this category include the total number of machine learning instances in

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

production, average number of new machine learning client wins per year, client retention rate, and client reference checks on the vendor's reputation in the market.

CLIENT SERVICE

ACI, Brighterion, and Featurespace all did particularly well in the client service category. Client ratings of the vendors' service and support, responsiveness, ability to deliver on promises, and cost-to-value ratios were the primary drivers of the ratings in this category, along with the vendor's position on key support items, such as providing 24/7 support, having a dedicated point of contact, facilitating customer advisory boards, and offering global/localized support.

PRODUCT FEATURES

Given the complexity of machine learning platforms and the wide variety of use cases and market needs that they must serve, it's unsurprising that no vendor checked all of the boxes for product features. Feedzai edged out the rest with the highest score in this category, followed by Featurespace, Brighterion, and Simility.

THE AIM RECOGNITION

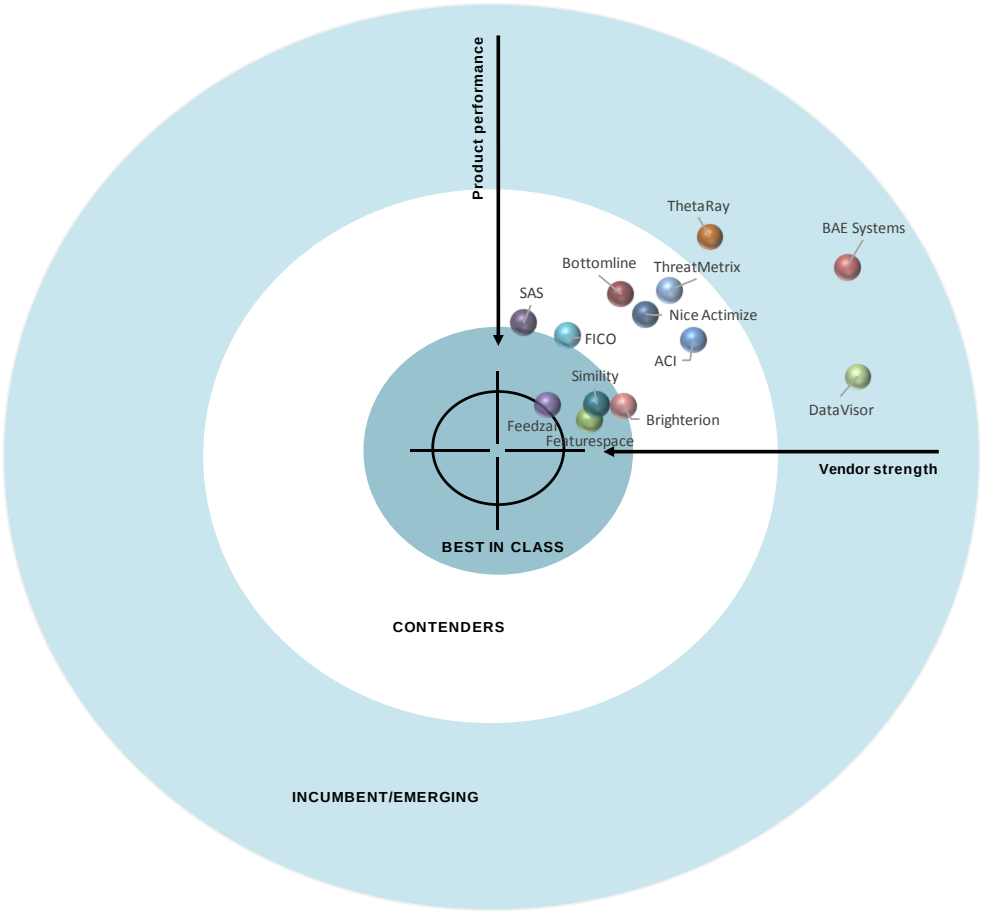
To recap, the final results of the AIM recognition are driven by three major factors:

- Vendor-provided information based on Aite Group's detailed AIM RFI document
- Participating vendors' client reference feedback and/or feedback sourced independently by Aite Group
- Analyst analysis based on market knowledge and product demos provided by participating vendors

Figure 18 represents the final AIM evaluation, highlighting the leading vendors in the market.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

Figure 18: Fraud and AML Machine Learning Platform AIM



Source: Aite Group

BEST-OF-BREED VENDORS: FEEDZAI, FEATURESPACE, AND SIMILITY

Featurespace, Feedzai, and Simility all emerge as best in class. All three vendors are among the new generation of entrants to the market and score high marks for the completeness of their product offerings, model performance, and the firms' responsiveness and support capabilities.

LEADERS OF THE CONTENDERS: FICO, SAS, AND BRIGHTERION

Long-standing market players FICO and SAS are joined by Brighterion as the leaders of the contenders. All of these vendors' scores have them right on the cusp of the best-of-class category.

MOST SCALABLE PLATFORM

Brighterion's scalability is over twice that of its closest competitor in this regard, boasting 62,000 TPS in production. Its streaming infrastructure with no underlying databases is a key driver of this impressive performance.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

VENDOR PROFILES

This section provides profiles of vendors that have participated in this AIM evaluation.

ACI WORLDWIDE

ACI Worldwide (ACI) powers electronic payments and banking for more than 5,100 organizations around the world. The firm has more than 40 years of payments expertise and customers in more than 80 countries, including 18 of the top 20 banks worldwide, more than 300 leading global retailers, and more than 1,500 banks, financial intermediaries, and merchants using ACI's fraud prevention solutions. ACI's UP Proactive Risk Manager (PRM) solution is designed to combat existing and emerging fraud threats using a combination of fraud and payments data and advanced analytics. One of ACI's key value propositions in the financial crime arena lies in its tight integration between PRM and ACI's payments engines, connecting fraud insight from across the payments ecosystem for better and more efficient decisions.

AITE GROUP'S TAKE

ACI enables machine learning for its PRM clients as follows:

- **Custom machine learning models:** ACI can implement custom machine learning algorithms in the production PRM Scoring Engine. These models are capable of scaling to 5,000 TPS with sub-50 millisecond latency. Three of the algorithms are a sparse kernel method, a proprietary neural network, and a dimensionality expansion method. ACI's data scientists leverage ACI's library of thousands of fraud features, developed over more than 40 years of supporting FIs' financial crime mitigation efforts.
- **Native model-builder capability:** PRM includes the ability to create adaptive machine learning models within the standard product. ACI's global team of fraud consultants provide training and templates on how to create and maintain adaptive machine learning models that typically follow logistic regression along with weight-of-evidence methodologies. Model templates provided are based on the different payment channels along with enterprise models (for cross-enterprise analysis and tactical models focused on specific segments (e.g., ATM, CNP, online banking).
- **Import via PMML:** PRM can support the import of third-party or bank-developed models via PMML and incorporate these for real-time or post-real-time decision-making.

In-market use cases include payment card fraud and online banking fraud. ACI also offers clients an embedded ability to send two-way text messages, push notifications, and communication via email and interactive voice response to consumers to help enable speedy resolution to alerts.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

BASIC FIRM AND PRODUCT INFORMATION

- **Headquarters**: Naples, Florida
- **Founded:** 1975
- **Number of employees**: More than 3,900
- **Ownership**: Nasdaq: ACIW
- **Percentage of revenue invested in R&D:** More than 15%
- **Product name:** UP Proactive Risk Manager (PRM)
- **Target customer base for PRM**: Financial institutions and processors
- **Modeling:**
  - **Citizen-data-scientist enablement?** Yes
  - **Vendor-developed and maintained models?** Yes
  - **Support for import of external models?** Yes
- **Implementation options**: On premises, private cloud, vendor-hosted, or public cloud (AWS, Azure, or Google)
- **Average new machine learning client wins per year over the past three years:** Two
- **Next release date**: September 2019

TOP THREE STRATEGIC PRODUCT INITIATIVES COMPLETED IN THE PAST 12 MONTHS

- Multitenant functionality for processors and ACI's hosted platform—one instance of the software will allow multiple customers to operate PRM as if they were running separate instances
- Expanded support and functionality for real-time payments
- Expansion and simplification of the solution's ability to communicate with external systems through a services layer

TOP THREE STRATEGIC PRODUCT INITIATIVES IN THE NEXT 12 TO 18 MONTHS

- **Continuous learning and multiple model development workstreams:** ACI has defined multiple model development workstreams that will generate models and automate their deployment into the production PRM environment. Continuous learning is a roadmap initiative consisting of a new PRM module that will execute as an autonomous process with no human intervention within the production PRM environment. The following are the workstreams and their availability as an existing ACI professional service offering or a defined roadmap initiative:

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

  - **Machine learning research workstream:** The primary objectives of this workstream are higher model predictive performance and decreased model delivery time via the analysis, development, and productization of new machine learning algorithms, features, and data sources, as well as the introduction of the continuous-learning PRM module. Completed by machine learning researchers, the outputs of this workstream are new algorithms and features into the automated daily model workstream.
  - **Automated daily model workstream**: This workstream consists of the development and delivery of full portfolio and segment models within 24 hours. Full portfolio models are used to score all activity of the FI's target product (credit, debit, online banking, wire, etc.), and the segment models are developed on data segments having unique fraud and genuine patterns. Following automated model development, model deployment into the FI's production environment is fully automated with no need for intervention.
  - **Continuous learning:** The continuous learning module will update production model parameters with user-defined events, such as confirmed fraud as it imported into the PRM database, within minutes or seconds of the event. The continuous learning module will update both the primary portfolio models generated in the model development workstream and segment models.

- **Next-generation machine learning algorithms**: ACI is investing in the machine learning algorithms that are core to PRM fraud detection. The algorithms its data science researchers are designing are capable of representing much higher dimensionality feature subsets while still providing all the benefits of its existing suite of algorithms. In addition, its researchers are extending the machine learning algorithms, which are used during the model development process, separate from those in production, for purposes such as ensemble model generation, model optimization, and the use of simple models as inputs to more complex production models.

- **Automated feature engineering**: ACI's existing feature engine is capable of assimilating many data elements across a wide variety of time windows, capturing key genuine and fraud account-holder behaviors and representing these to the models. ACI has been investing in greater automation of the feature generation process, and the firm will extend this automation as part of this roadmap initiative. This increased feature engineering automation will increase the rate of new feature development and evaluation, and will continue to be complemented by the human expert integrating targeted payments and fraud patterns across all action levels (card, account, terminal, ATM, etc.). This will be further complemented by the extended stream analytics and complex event processing capabilities coming in future releases of the platform.

CLIENT FEEDBACK

ACI's client references were universally complimentary of PRM's flexibility. PRM's users have the ability to create any fraud strategy they want for any payment type using any data element available to the solution. PRM provides clients with the ability to easily use other systems'

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

features and functions as well as the ability to link PRM to other databases. The speed of the system is also highlighted as a strength—use cases that client references are using PRM for include payment card and online banking fraud mitigation, which require support for high throughput with low latency.

While the ability of the case management system to aggregate alerts at the client level rather than the alert level was highlighted as a strength, other aspects of the UI, such as look and feel as well as the workflow efficiency, are on clients' wish list for improvement.

Other areas of improvement that clients would like to see include system stability and code quality. In the words of one executive interviewed, "With great flexibility comes instability. PRM is more unstable than many of our other systems." In another executive's words, "There are new releases every six months or so, and quite a few defects. They seem to steer away from ownership there, which just extends time to resolution." ACI is responding to this market feedback and has taken steps to reduce the number of major and point releases it puts out annually.

Table L provides a summary of PRM's strengths and improvement opportunities.

Table L: Key Strengths and Improvement Opportunities—ACI Worldwide

Strengths	Improvement opportunities
Tight integration between PRM and ACI's payments engines	System instability and code quality
System flexibility	Look, feel, and efficiency of the UI
Embedded risk intervention capabilities	

Source: Aite Group

BAE SYSTEMS

BAE Systems is a British defense and security company. Its NetReveal product suite provides clients in 90 countries with solutions in the areas of fraud, AML, and cybersecurity. BAE Systems' target market for its financial crimes product suite include Tier-1 and Tier-2 FIs.

AITE GROUP'S TAKE

BAE Systems provides the ability for its NetReveal clients to add machine learning detection routines in the following ways:

- **Managed Analytics Service:** Through its Managed Analytics Service, clients can leverage BAE Systems' data science team to help build and maintain custom models on a professional services basis. The resulting models can then be deployed in NetReveal via PMML.
- **Advanced Analytics Platform:** The NetReveal Advanced Analytics Platform (AAP) is an add-on to the NetReveal detection engine to enable clients' data scientists and/or data analysts to build custom machine learning models themselves. The AAP

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

provides the full suite of solutions that help with feature identification and creation of machine learning models using a variety of different algorithms (e.g., logistic regression, random forests, gradient boost, neural networks), then facilitates side-by-side comparisons of model performance using the client's historical data. Once the client has identified the optimal model configuration, the model can be deployed in NetReveal using PMML.

- **Import of third-party models:** NetReveal can support the import of third-party or bank-developed models via PMML.

In-market use cases leveraging BAE Systems' machine learning capabilities include electronic payments, online banking, and application fraud detection.

BASIC FIRM AND PRODUCT INFORMATION

- **Headquarters**: London
- **Founded:** 1999
- **Number of employees**: 83,500
- **Ownership**: OTC: BAESF
- **Percentage of revenue invested in R&D:** 10% or less
- **Target customer base**: Financial institutions, processors, insurance carriers
- **Modeling:**
  - **Citizen-data-scientist enablement?** Yes
  - **Vendor-developed and maintained models?** Yes
  - **Support for import of external models?** Yes
- **Implementation options**: On premises, private cloud, or public cloud (AWS and Azure)
- **Product names:** NetReveal Advanced Analytics Platform and NetReveal Payments Fraud, NetReveal AML Parameter Optimization, AML Transaction Monitoring Optimization
- **Target customer base for the Advanced Analytics Platform**: FIs, issuing processors, and insurance carriers
- **Average new machine learning client wins per year over the past three years:** Two
- **Next release date**: April 2019

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

TOP THREE STRATEGIC PRODUCT INITIATIVES COMPLETED IN THE PAST 12 MONTHS

- The tool's ease of use for the end user
- Full big-data support
- Pluggable architecture to support additional third-party machine learning libraries

TOP THREE STRATEGIC PRODUCT INITIATIVES IN THE NEXT 12 TO 18 MONTHS

- Model governance
- Active learning
- Integration of lightweight network analytics

CLIENT FEEDBACK

One of BAE Systems' reference clients is an automated clearinghouse using the system for analysis of electronic payments activity at the national level. The scalability of the system to handle its real-time detection and alerting needs at a large volume was highlighted as a key strength by this client.

Model performance was also highlighted as a strength by BAE Systems' clients, although time to market for BAE Systems' custom-developed models was cited as a challenge. In the words of the client interviewed, "The models do well once they get in there, but time to market is too long for fraud especially. Last time around, it took BAE Systems six weeks to build the model and two weeks to deploy."

Another challenge cited by one interviewee is getting data into the system in a way that it can be consumed and analyzed—the version of the platform that this FI is on makes it difficult to write rules off data that is already in the system (e.g., ZIP code), and it also presents challenges when the FI wants to stream new data in from its mobile banking app.

The UI was also flagged as an area for improvement. In the words of one executive, "The UI needs to be upgraded to address the expectation for a seamless user experience. While this is a banking application, our analysts' expectations are shaped by their consumer experiences." This client made a few customizations to the UI but said that there is a lot of hard coding, which limits the customization opportunities.

Table M provides a summary of BAE Systems' strengths and improvement opportunities.

Table M: Key Strengths and Improvement Opportunities—BAE Systems

Strengths	Improvement opportunities
Model performance	Ease of data consumption
Scalability to process a large volume of data	User interface

Source: Aite Group

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

BOTTOMLINE TECHNOLOGIES

Bottomline Technologies (Bottomline) has been an innovator in business payment automation technology for 30 years. Bottomline helps simplify and secure complex business payments for thousands of companies in 92 countries. Bottomline acquired the Israel-based firm Intellinx in 2015 to add a financial crime mitigation component to its payment solutions.

AITE GROUP'S TAKE

Bottomline's machine learning solution is an add-on module that can be combined with its CFRM or its Secure Payments products. It employs an open architecture that supports algorithms from Apache Spark and Google TensorFlow. In addition, the system includes Bottomline's proprietary DensiCube algorithm, which relies on clustering techniques, and can support supervised, unsupervised, or semisupervised machine learning. Bottomline can enable automatic generation of models as well as controlled generation by a data scientist through a dedicated UI. The Bottomline machine learning module can also support model creation with external algorithms such as R or Python.

The DensiCube supervised learning creates clusters of the positive and negative classes of the target variable. Each new data point is then scored against the clusters, and the best result is returned (closest to a positive or negative cluster, which one, and how close). Unsupervised learning recognizes all the data as a single class, then fills in the space around the data points with evenly spaced synthetic negative points. A model that best defines the edges of the positive class is built. New data points are then scored by distance to all of the clusters, and the closest is returned with the score of how close. The system supports segmentation so that unique models can be automatically created based upon a specified segmentation feature. This allows large-grained segmentation, such as separating business from consumer, or finer-grained segmentation that can model down to a segment of one.

In-market machine learning use cases include ACH, wire, and SWIFT fraud, internal fraud, and healthcare fraud detection. The solution can be expanded to other types of fraud in implementation. Bottomline's machine learning module provides human-readable explanations to the investigator as part of transaction scoring.

BASIC FIRM AND PRODUCT INFORMATION

- **Headquarters**: Portsmouth, New Hampshire
- **Founded:** 1989
- **Number of employees**: 1,700
- **Ownership**: Nasdaq: EPAY
- **Percentage of revenue invested in R&D:** 18%
- **Product names:** Cyber Fraud & Risk Management (CFRM), Secure Payments
- **Target customer base for CFRM and Secure Payments**: Financial institutions, healthcare, and corporations

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

- **Modeling:**
  - **Citizen-data-scientist enablement?** Yes
  - **Vendor-developed and maintained models?** Yes
  - **Support for import of external models?** Q3 2019 roadmap
- **Implementation options**: On premises, private cloud, vendor-hosted, public cloud (AWS, Azure, Google)
- **Average new machine learning client wins per year over the past three years:** 50
- **Next release date**: May 2019

TOP THREE STRATEGIC PRODUCT INITIATIVES COMPLETED IN THE PAST 12 MONTHS

- Open algorithms supporting Apache Spark, Google TensorFlow, and third-party extensibility
- User friendly, spreadsheet–like data transformation user interface that supports real-time feature engineering (including numeric, string, and statistics functions) and includes intelligent transformation (such as natural language processing, reference data enrichment, and ambiguous date/address resolution)
- Automatic model generation and tuning, which includes feature selection and reduction, multiple model iteration generation, and automatic selection of the best model

TOP THREE STRATEGIC PRODUCT INITIATIVES IN THE NEXT 12 TO 18 MONTHS

- Further enhancements to auto-tuning to automatically perform feature engineering; for example the system will be able to analyze whether a transaction amount should be averaged, compared against standard deviation, and decide the appropriate time window for the aggregate (seven days/ 30 days, quarterly, etc.)
- Ad hoc visual analysis of data allowing the data scientist to explore the input data and the models
- Enhancements to enable the system to acquire data directly from web data sources and extract meaningful features that can be used by a model.

CLIENT FEEDBACK

Bottomline's client references are complimentary of the solution's flexibility and customizability. The firm also receives high marks for its responsiveness to service and support requests. In terms of areas needing improvement, a top wish-list item is support for additional fraud use cases.

Table N provides a summary of Bottomline's strengths and improvement opportunities.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

Table N: Key Strengths and Improvement Opportunities—Bottomline Technologies

Strengths	Improvement opportunities
Service and support	Support for additional out-of-the-box use cases
Expertise with ACH, wire, and SWIFT fraud use cases	
Ability to provide vendor-trained models and to support client-developed models	

Source: Aite Group

BRIGHTERION

Brighterion, a Mastercard company, offers a portfolio of AI and machine learning technologies to mitigate AML, acquiring fraud, omnichannel fraud, collections, and credit risk for FIs, governments, and healthcare organizations. Its AI platform enables discovery, identification, and mitigation of anomalous activities.

AITE GROUP'S TAKE

Brighterion's solution is based on a distributed architecture to optimize performance, scalability, and resilience to disruption. Its models employ a combination of unsupervised and supervised analytics, and average a response time of less than 10 milliseconds, with 6,200 TPS throughput. The system accepts real-time streaming data and does not require a database. In-market fraud and AML use cases include payment card fraud, sanctions screening, breach and network-level anomaly detection, and omnichannel fraud detection.

Brighterion's patented modeling approach applies a combination of 10 machine learning techniques to understand behavior and flag anomalies. It anchors its technology around smart agents, each of which tracks and adaptively learns behavior at the segment-of-one level. The models can ingest both structured and unstructured data, and apply both supervised and unsupervised modeling techniques to create profiles specific to each entity, establish baseline normal behavior, and rapidly flag anomalous behavior, both at the individual and cohort level.

Brighterion can handle the model creation and deployment, and it also provides the interfaces to support creation of custom models within its platform. Its patented modeling engine automatically discovers important features and associations, creates new fields, and enriches the data. It automatically builds and tests millions of machine learning models in parallel, then merges the models together to create the optimal, production-ready models that can continue to iteratively learn.

BASIC FIRM AND PRODUCT INFORMATION

- **Headquarters**: San Francisco
- **Founded:** 2000
- **Number of employees**: 65

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

- **Ownership**: Wholly owned by Mastercard
- **Percentage of revenue invested in R&D:** More than 50%
- **Product name:** Brighterion AI Platform
- **Target customer base**: Financial institutions, processors, government, and healthcare firms
- **Implementation options**: On premises or vendor-hosted; public cloud is on its 2019 roadmap
- **Modeling:**
  - **Citizen-data-scientist enablement?** Yes
  - **Vendor-developed and maintained models?** Yes
  - **Support for import of external models?** Yes
- **Average new machine learning client wins per year over the past three years:** 20
- **Next release date**: Q4 2019

TOP THREE STRATEGIC PRODUCT INITIATIVES COMPLETED IN THE PAST 12 MONTHS

- Two new types of unsupervised learning algorithms
- New types of workflows in case management
- Consumption and display of unicode data (e.g., Chinese, Arabic)

TOP THREE STRATEGIC PRODUCT INITIATIVES IN THE NEXT 12 TO 18 MONTHS

- Brighterion plans to release a new version of its unsupervised learning platform.
- "Textual reasoning" describes Brighterion's patented ability to receive and analyze millions of simultaneous text and/or voice messages. Each word is contributed to a qualia generator that spawns the word into its possible contexts, themes, or other reasonable ambiguities that can exist at the level of sentences, paragraphs, and missives. Once the context of a whole missive has been predicted, each paragraph is deconstructed into subcontexts that are appropriate within the overall theme. Particular contexts identified are then useful to trigger an actionable output.
- Brighterion plans to release a new version of its AML solution through the application of Smart-Agents technology to AML use cases.

CLIENT FEEDBACK

Brighterion receives high marks from its client references for the system's performance and scalability. One of Brighterion's client references runs the system in a multitenant environment

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

with 18 to 21 models running concurrently, replicated across 20 clusters, producing tens of thousands of real-time decisions per second. The models' performance is also highlighted as a key strength. Whereas traditional models that are only refreshed every 12 to 24 months aren't able to respond quickly to new threat or commerce patterns, Brighterion's system is able to infuse adjustments into the model on an ongoing basis. As a result of this flexibility, the client reference that is running Brighterion in a multitenant environment has seen improvements in performance over time, with a 40% increase in detection and a 50% decrease in false positives.

The firm's willingness to customize its offering to its clients' needs and its can-do attitude are also highlighted by client references. One client notes Brighterion's willingness to delve into net new use cases, such as sanctions screening, and develop a solution that is not only effective but also acceptable to regulators, which is no small task with AML use cases.

In terms of areas of improvement, the UI is highlighted in reference interviews as an area of opportunity. In the words of one client, while it's functional, it needs updating both from a look-and-feel perspective and from a workflow perspective. Keeping up with the company's success is also a challenge that was highlighted in the reference interview—in the wake of its acquisition by Mastercard, the company's growth has accelerated, and its service and support capabilities have not kept pace. While Brighterion still receives fairly high marks for service and support, one of the reference clients says that it'd been waiting on data for several weeks post-upgrade; while it used to get responses to support requests within a day, post-acquisition the average response time has slipped to three days.

Table O provides a summary of client feedback on Brighterion's strengths and improvement opportunities.

Table O: Key Strengths and Improvement Opportunities—Brighterion

Strengths	Improvement opportunities
Scalability	Customer interface needs updating from both a look-and-feel perspective and a workflow optimization perspective
Model performance and adaptability	Service and support staffing to keep pace with company growth
Willingness to customize to clients' needs	

Source: Aite Group

DATAVISOR

DataVisor's mission is to leverage digital intelligence to protect and restore trust online. It partners with the some of the largest financial and internet properties such as Pinterest, Yelp, Ping An Insurance, and large banks in the U.S. and Asia to protect them from a wide array of attacks, including fraud, abuse, and money laundering, using a combination of machine learning analytics and DataVisor's proprietary Global Intelligence Network. The company is headquartered in Mountain View, California, with offices in Shanghai and Beijing.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

AITE GROUP'S TAKE

DataVisor utilizes a combination of unsupervised and supervised modeling techniques to help firms detect patterns of fraud and money laundering. The unsupervised routines combine clustering techniques with graph analysis to uncover suspicious patterns in unlabeled data. Unsupervised techniques have a great deal of benefit in that they can detect emergent fraud and money laundering patterns more quickly than supervised models. In the highly regulated FI environment, however, regulators still have a heavy emphasis on model explainability, and there is a perception among regulators that this transparency is harder to achieve with unsupervised techniques. The recent statements from U.S. regulators encouraging FIs to use more advanced analytic techniques is a positive sign that there may be more openness to unsupervised analytics in the financial sector in the near future.

DataVisor's Global Intelligence Network is another key value driver. DataVisor's system aggregates truth and reputational data associated with IP addresses, geolocation, email domains, mobile device types, operating systems, browser agents, phone prefixes, and more. By analyzing the connections between these data points, DataVisor is able to provide fine-grained signals and reputation scores to enhance detection.

While today all of the models are built and maintained by DataVisor, the March 2019 release will include a capability to enable the clients' citizen data scientists to build and deploy their own models within the system.

BASIC FIRM AND PRODUCT INFORMATION

- **Headquarters**: Mountain View, California
- **Launched in:** 2014
- **Number of employees**: More than 130
- **Ownership**: Sequoia Capital China, Genesis Capital, GSR Ventures, and New Enterprise Associates
- **Percentage of revenue invested in R&D:** More than 15%
- **Product name:** DCube
- **Target customer base**: Financial institutions, e-commerce merchants, and social media
- **Implementation options**: On premises, public cloud (AWS, Azure, and Google), or private cloud
- **Average new machine learning client wins per year over the past three years:** Undisclosed
- **Next release date**: Not applicable, full SaaS environment, does not use external versioning

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

TOP THREE STRATEGIC PRODUCT INITIATIVES COMPLETED IN THE PAST 12 MONTHS

- Enhanced data integration capability to connect to data across databases and sources in both cloud and on-premises environments
- Client-configurable unsupervised machine learning model tuning, along with advanced attack analytics and UI capabilities, giving end users the ability to mine and surface insights within the UI
- Improved investigation and case management interfaces

TOP THREE STRATEGIC PRODUCT INITIATIVES IN THE NEXT 12 TO 18 MONTHS

- Extend functionalities for both risk and data science teams to enable more control, transparency, and streamlined workflow
- Enhance product suite capabilities to build a more comprehensive fraud solution, including support for building customized features, supervised learning models, unsupervised learning models, and advanced rules engines with the ability to ensemble results in a decision engine
- Expand fraud detection solution to adjacent verticals (telecom, insurance, government)

CLIENT FEEDBACK

DataVisor scored excellent marks from its client references for its service, support, and willingness to go the extra mile. The clients interviewed say that everyone they work with at DataVisor is very responsive and brings a can-do attitude. One interviewee also likes the fact that DataVisor doesn't display arrogance or overpromise—the DataVisor team genuinely partners to respond to customers' requests for improvements and enhancements.

From a performance perspective, clients say that DataVisor's analytics are good at detecting similar mass events (e.g., robotic attacks, ring-based attacks). Where clients would like to see improvement is in the patiently nurtured fraud, from both a new account and ATO perspective—they'd like to see DataVisor focus on improving its analytics to detect one-off fraud. Table P provides a summary of client feedback on DataVisor's strengths and improvement opportunities.

Table P: Key Strengths and Improvement Opportunities—DataVisor

Strengths	Improvement opportunities
Good at detecting clustered attacks that are similar	Detection of patiently nurtured frauds and nonautomated, one-off attacks
Very responsive, can-do attitude, great at hand-holding clients	Use of unsupervised techniques creates an uphill battle in the FI model governance climate
Unstructured data analytics	

Source: Aite Group

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

FEATURESPACE

The technology behind Featurespace's adaptive behavioral analytics technology was created at Cambridge University in the late 2000s. Since that time, Featurespace's ARIC platform has helped FIs, processors, and gaming firms around the globe with their financial crime challenges.

AITE GROUP'S TAKE

Featurespace's ARIC platform produces machine learning models using its own proprietary Bayesian analytics-based approach, or the client can import third-party models via PMML or data studio products such as H2O. In-market use cases include payment card fraud, application fraud, and holistic cross-channel, cross-product customer risk scoring.

The platform consists of a three-tiered architecture. The API tier includes the API for data ingestion and the UI. The ARIC platform has been designed for high availability, resiliency, and easy integration with other systems (a good example of this is a banking customer with 81 data feeds into its ARIC system for real-time fraud mitigation). The platform can support multitenancy, with model customization capabilities at the subtenant level.

Transactions are posted to a RESTful API service, and the risk scores are included in the API response. This tier also contains the UI in which users interact for alert management, analytical configuration, reporting, and general administration. The processing tier runs inside a complex event processing framework, takes the messages from the internal message queue, and executes Bayesian models and business rules, producing scores and making decisions. The database tier stores all of the profiles and data required for the ARIC engine. While ARIC employs both supervised and unsupervised modeling techniques, a supervised machine learning algorithm is used as the final scoring mechanism. The system is built to handle thousands of events per second with millisecond response times.

BASIC FIRM AND PRODUCT INFORMATION

- **Headquarters**: Cambridge, U.K.
- **Launched in:** 2008
- **Number of employees**: 200
- **Ownership**: Highland Europe, Nesta Ventures, TTV Capital, IP Group, Insight Venture Partners, MissionOG, Worldpay, and angel investors
- **Percentage of revenue invested in R&D:** Greater than 15%
- **Product name:** ARIC
- **Target customer base**: Financial institutions, issuing and acquiring processors, and insurance and gaming firms
- **Modeling**
    - **Citizen-data-scientist enablement?** No
    - **Vendor-developed and maintained models?** Yes

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

    - **Support for import of external models?** Yes
- **Implementation options**: On premises, private cloud, or public cloud (AWS, Azure, and Google)
- **Average new machine learning client wins per year over the past two years:** 8.5
- **Next release date**: Q1 2019

TOP THREE STRATEGIC PRODUCT INITIATIVES COMPLETED IN THE PAST 12 MONTHS

- **Multitenancy with customizable models:** As an enterprise platform, multitenancy enables Featurespace clients to either resell the ARIC fraud-prevention capabilities to their customers or service discrete business units across an organization from a single deployment. Tenants within the platform can benefit from shared intelligence and individual models optimized for their use case.
- **Platform resiliency and monitoring:** Featurespace's clients rely on the platform for mission-critical business applications 24 hours a day, seven days a week. To ensure the firm meets the expectations of its customers, it continues to invest engineering effort to maintain a reliable, robust, and secure platform.
- **Active-active disaster recovery:** Featurespace's ARIC platform is deployed in an active-active configuration, which ensures that any data center outage will not impact the platform's ability to provide continuous fraud protection for its clients.

TOP THREE STRATEGIC PRODUCT INITIATIVES IN THE NEXT 12 TO 18 MONTHS

- **Advanced analytics:** Providing its customers' data science teams with additional tools and functionality to create their own models
- **Behavioral biometrics:** Incorporating and visualizing a consumer's on-device behavior as part of risk decision and investigation
- **Identity-as-a-service:** Orchestrating third-party API call-outs

CLIENT FEEDBACK

All the Featurespace clients interviewed for this report are complimentary of the platform's performance as well as the firm's professionalism and support ethos. One of the selling points for one of the U.S.-based FIs using the Featurespace system was the firm's European roots and existing install base; since many fraud trends tend to hit Europe a few years before they come to the U.S. (e.g., post-EMV fraud migrations, real-time payments fraud), Featurespace was already solving problems that banks in the U.S. hadn't seen yet.

According to one of the issuer references, Featurespace's Bayesian inference analytics are strong at detecting its payment card fraud (in particular CNP fraud and contactless fraud) with a low false-positive rate. The initial POC provided results that were head and shoulders above others tested, and these results have been borne out in production, with a 63% reduction in false

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

positives and a 177% increase in CNP fraud detection. A large merchant acquirer provides similar feedback, saying Featurespace significantly outperformed four other leading machine learning platform vendors in a head-to-head value test based on a year's worth of transactional data.

In terms of areas needing improvement and desired enhancements, one of the banks would like to see the management dashboard provide more flexibility—the default Featurespace interface uses number of alerts, rather than number of incidents, as the basis for KPI calculations, so the FI has to do extra work outside the system to get to the types of KPIs it wants to track. Another FI would like to see Featurespace branch out to use more unsupervised analytics for select use cases, such as chip card fraud, which has less training data.

Table Q provides a summary of client feedback on Featurespace's strengths and improvement opportunities.

Table Q: Key Strengths and Improvement Opportunities—Featurespace

Strengths	Improvement opportunities
Strong model performance	More use of unsupervised techniques for select use cases
Excellent service and support, both during implementation and ongoing	Greater flexibility in UI to configure KPIs to the clients' desired form of metrics tracking

Source: Aite Group

FEEDZAI

Feedzai was founded by data scientists and aerospace engineers with the mission of making banking and commerce safe. The world's largest banks, payment providers, and retailers use Feedzai's machine learning technology to manage the risks associated with banking and shopping, whether it's in person, online, or via mobile devices.

AITE GROUP'S TAKE

Feedzai's platform combines a flexible range of model development and deployment mechanisms with in-memory, event-streaming technology to detect fraud and money laundering activities in real time. Feedzai recognizes the diverse range of data science expertise, resources, and client needs across the financial services industry, so the platform provides a variety of ways that firms can leverage and deploy its capabilities—empowering the data scientists at firms to build their own models, enabling import of third-party models, and providing professional services resources to build custom models for its clients. In-market use cases include payment card fraud, application fraud, wholesale transactional fraud, AML, and analysis of open-API traffic for anomalies.

The platform is built on top of big-data tools such as Spark, Cassandra, and Hadoop, along with proprietary code, which delivers low latency and high availability. Feedzai's analytics, which employ random forest, XGBoost, LightGBM, logistic regression, anomaly detection, gradient boosted machine, deep neural networks, and isolation forests algorithms, can model down to the individual and the cohort levels in real time and provide human-readable explanations with

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

the resulting alerts. Feedzai's platform can also support multitenancy, with model customization at the subtenant level.

Feedzai's AutoML capabilities enable data scientists to automate the feature generation process, which saves significant time in the model development and deployment process. AutoML also compares multiple modeling approaches on the same feature set on historical data and presents the client's data scientists with the metrics to select the optimal approach.

BASIC FIRM AND PRODUCT INFORMATION

- **Headquarters**: San Mateo, California
- **Founded:** 2009
- **Number of employees**: 394
- **Ownership**: Citi Ventures, Oak HC/FT, and Sapphire Ventures
- **Percentage of revenue invested in R&D:** 24%
- **Product names:** Transaction Fraud for Banks, Transaction Fraud for Acquirers and Processors, Account Opening, Anti-Money Laundering, Transaction Fraud for Merchants
- **Target customer base**: Financial institutions, large merchants, issuing processors, and acquiring processors
- **Modeling**
  - **Citizen-data-scientist enablement?** Yes
  - **Vendor-developed and maintained models?** Yes
  - **Support for import of external models?** Yes
- **Implementation options**: On site, private cloud, public cloud (AWS, Azure)
- **Average new machine learning client wins per year over the past three years:** 22
- **Next release date**: April 2019

TOP THREE STRATEGIC PRODUCT INITIATIVES COMPLETED IN THE PAST 12 MONTHS

- **Feedzai Genome:** Feedzai has developed an advanced detection system, giving fraud investigators and analysts an intuitive way to find and visualize complex financial crime patterns using machine learning and link analysis graph technology. Feedzai Genome automatically uncovers emerging fraud and AML patterns and improves the depth and efficiency of risk assessment by looking at transactions in groups instead of one by one, and matching emerging patterns of fraud to previously identified patterns.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

- **Feedzai OpenML:** Feedzai believes that data scientists can achieve better outcomes when they have the flexibility to experiment and innovate by building models in any language, using any library, and on any platform. Feedzai opened up its enterprise risk management platform to provide the flexibility to bring any existing or future external library or scoring frameworks via an API. This enables firms to choose the approach that delivers the best possible detection results for any given use case. OpenML offers data scientists three different ways to work with Feedzai: (1) train a Feedzai machine learning algorithm in Feedzai's platform, (2) train an external machine learning algorithm in Feedzai's platform, (3) import a model trained externally to Feedzai's platform. Feedzai OpenML also integrates with many common data science and machine learning languages, such as R and Python, and allows data scientists to leverage pre-written open-source machine learning libraries, such as H2O, Spark's MLlib, scikit-learn, and TensorFlow.

- **Feedzai AutoML**: Feedzai AutoML introduces a new timescale for data science work, replacing weeks of work with one-click models, allowing teams to generate thousands of new features in minutes, not weeks. It speeds up the process of building fraud prevention workflows by as much as 50 times, when compared to current time spent on feature engineering and model creation. With AutoML, Feedzai is freeing data scientists from the most repetitive and time-consuming steps of the data science process, allowing them to perform more consequential tasks.

TOP THREE STRATEGIC PRODUCT INITIATIVES IN THE NEXT 12 TO 18 MONTHS

- **Automation everywhere:** Feedzai's R&D is actively focusing on two automation advancements—auto-data preparation and auto-governance. These are critical in connecting the online and offline machine learning systems, as data scientists spend around 60% of their time integrating and preparing data for business usage. FIs need intelligent tools to handle data coming from new channels, new geographies, and new use cases in order to adapt to new regulations. The format, structure, and complexity of the data is varied and unpredictable. Feedzai's mission is to empower FIs to deal with any data in a fraction of the time with zero manual effort all while ensuring production systems and processes stay compliant by providing the appropriate automated tools.

- **Smarter detection and explainability:** While leveraging the power of AI to automate processes and decisions will increase efficiency, other advancements in detection and explainability need to happen in parallel to ensure accuracy. FIs need to be able to understand system behavior and outcomes to improve the speed and transparency of their decisioning. This becomes especially important for use cases such as AML, for which FIs need to have full transparency to assure regulators that they are compliant. This is an area that Feedzai has already actively invested in with its Whitebox Explanations, a proprietary algorithm that translates model decisions into simple, human-readable explanations that guide analysts, data scientists, and upper management in their decisioning. In 2019, Feedzai will focus on building the next generation of Whitebox Explanations, the Feedzai AI Interpreter. In addition to

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

expanding the Whitebox Explanations for new algorithms such as anomaly detection, deep learning, and external machine learning models, Feedzai will work on broadening the scope of explainability and transparency across all components. While explaining system and model decisions, Feedzai will actively monitor and explain the system's overall behavior as well as guide the user on next best actions. For example, the system will provide detailed alerts when there are sudden changes that, in aggregate, might indicate an attack. The system will also provide human-readable explanations for why a behavior is being identified as an attack, and it will provide clear recommendations on next steps. This will enable FIs to work with an autonomous tool to augment data scientists and analysts with recommendations they can trust transparently.

- **Segments-of-one profiling:** With Risk Ledger (federated data across its customer base and partners), Feedzai augments its existing profiles and equips each customer with a unique blend of its data and ecosystem-wide insights, enabling mitigation of attacks spanning multiple institutions. Powered by the global data, Feedzai's patent-pending algorithms, such as automatic detection of points of compromise, will reveal hidden connections, traces and origins of ATM skimming, bots, and other attacks. To stay several steps ahead of fraudsters, Feedzai aims to employ deep learning and anomaly detection technologies, helping data scientists and fraud analysts to go beyond what they can predict or model about fraudulent behavior.

CLIENT FEEDBACK

All of the Feedzai clients interviewed for this report had conducted rigorous multivendor selection processes that included both long-time industry players and newer firms. Feedzai came out on top in all of these evaluations. Two of the clients did not want a vendor with black-box analytics, and the transparency of Feedzai's approach was a key decision criterion. Clients are also complimentary of Feedzai's innovative approach to machine learning and the platform's ability to empower the bank's data scientists' custom model development efforts.

The scalability of Feedzai's offering to support a high volume with low latency as well as the platform's ability to crunch an enormous amount of data from multiple touch points are also cited as key strengths by a couple of the executives interviewed. In one bank executive's words, "Feedzai was built from ground up with scalability and big data in mind, versus others who are trying to adapt legacy technology to bring these in."

Feedzai's service and support are also a source of client satisfaction. One FI executive says that Feedzai has "a great bunch of people to work with—they over deliver, are very eager, and bring a lot of knowledge to the table." Another client comments on Feedzai's tight integration between product and delivery teams, which helps with speedy problem solving. This synergy is not always the case with other vendors.

In terms of areas in which clients would like to see improvement or enhancement, the number one request from one of Feedzai's large bank clients is enhancements to the case management system. The executive characterizes the existing functionality as generic, and the FI needs it to be more flexible while having more enforceable governance controls (e.g., configurable 2/4/8 eye approvals depending on the actions being taken). Another wish-list item is embedded end-user

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

authentication (e.g., two-way text) to enable real-time communication with consumers for resolution of alerts.

Table R provides a summary of Feedzai's strengths and improvement opportunities.

Table R: Key Strengths and Challenges—Feedzai

Strengths	Improvement opportunities
Scalability	Embedded end-user authentication capabilities
Responsive service and support	More robust case management
Comprehensive machine learning platform that can empower model building, support the import of external models, and leverage Feedzai resources for custom model building	

Source: Aite Group

FICO

FICO is a leading analytics software company and the pioneer of neural network technology. It helps businesses in more than 80 countries make better decisions that drive higher levels of growth, profitability, and customer satisfaction. FICO provides analytics software and tools used across multiple industries to manage risk, fight fraud, build more profitable customer relationships, optimize operations, and meet government regulations. Falcon is one of FICO's flagship products and is used by more than 10,000 FIs globally.

AITE GROUP'S TAKE

Falcon provides a portfolio of supervised, unsupervised, and semisupervised machine learning techniques that enable cross-channel, real-time behavioral profiling to separate legitimate and fraudulent financial transactions. The methods are developed and vetted by FICO's data science experts with extensive financial crime domain knowledge. FICO applies the optimal analytic technique for each type of fraud use case rather than using a one-size-fits-all approach to model development. Falcon also includes a consortium intelligence capability that incorporates billions of anonymized payment details from a global consortium of 10,000 contributing institutions.

Thanks to decades of processing in the high-volume payment card environment with its sub-half-second response time requirements, Falcon's platform is highly scalable, supporting over 20,000 TPS. Falcon employs a component-based architecture, in which the database and application server can be split onto different machines separate from the scoring server. This enables setups that include clustered application servers or databases and allow them to scale separately as needed.

FICO is one of the few vendors in this AIM evaluation that includes a native risk intervention capability. Thanks to FICO's 2012 acquisition of Adeptra, Falcon offers businesses an embedded ability to communicate with customers in real time using voice, SMS, mobile apps, and email. By contacting customers instantly using their preferred channel, firms can immediately resolve

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

important matters, such as identifying whether a credit transaction is fraudulent or giving the customer a path to resolution if it's a false positive.

The Falcon platform does not incorporate native model-building technology for FIs that want an environment that enables their citizen data scientists to build models within the platform.

BASIC FIRM AND PRODUCT INFORMATION

- **Headquarters**: San Jose, California
- **Founded:** 1956
- **Number of employees**: 3,800
- **Ownership**: NYSE: FICO
- **Percentage of revenue invested in R&D:** 11% to 15%
- **Product name:** Falcon
- **Target customer base for Falcon**: Financial institutions and issuing processors
- **Modeling:**
  - **Citizen-data-scientist enablement?** 2019 roadmap
  - **Vendor-developed and maintained models?** Yes
  - **Support for import of external models?** Yes
- **Implementation options**: On-site, private cloud, public cloud (AWS), or vendor hosted (FICO Analytics Cloud)
- **Average new machine learning client wins per year over the past three years:** 15
- **Next release date**: May 2019

TOP THREE STRATEGIC PRODUCT INITIATIVES COMPLETED IN THE PAST 12 MONTHS

- Ability for clients to deploy third-party and/or in-house-developed analytic models within Falcon
- Falcon executive dashboards that allow users to track KPI trends and underlying details in order to evaluate performance and optimize fraud-prevention strategies
- Semisupervised, self-calibrating machine learning models for retail banking and real-time payments fraud

TOP THREE STRATEGIC PRODUCT INITIATIVES IN THE NEXT 12 TO 18 MONTHS

- **Falcon X:** Falcon X is a cloud-based financial crimes solution that supports efficient operations across both fraud and compliance with open-source machine learning

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

analytics, unified case management, and flexible workflows that easily connect to keep pace with changing payment innovations. It will provide the ability to ingest all data types while performing real-time aggregations and variable calculations in order to stop financial crimes faster. Clients can choose from a wide range of proven, FICO-developed machine learning models or build their own models using open-source programming languages available in the FICO Financial Crimes Studio.

- **Model and rule simulation:** FICO is rolling out new benchmarking capabilities that will allow clients to compare their fraud detection performance metrics against those of other FIs. Available via a cloud-based portal and powered by the Falcon Intelligence Network, these benchmarks will serve as a global source of comparative machine learning performance measures. In 2019, these capabilities will be extended to include the ability for clients to simulate outcomes based on changes to underlying rules and models. With billions of accounts and tagged outcomes from more than 10,000 FIs, the Falcon Intelligence Network spans cards, CNP transactions, person-to-person transfers, and mobile payments.
- **Real-time AML analytics:** AML technologies are ripe for an overhaul, with machine learning leading the way. FICO has invested heavily in new analytical techniques designed to reduce the cost burden of false positives while improving detection rates. A core tenet of these techniques is advances in explainable AI. These advances, which will be available in Falcon X, help humans better understand how machine learning models derive a score. As a result, model shelf life will increase, and organizations will be able to apply machine learning in ways that conform to governance and regulatory requirements that surround compliance strategies.

CLIENT FEEDBACK

FICO has a strong reputation for analytical modeling, and most of the client reference interviews reinforced that model performance as a point of satisfaction. One of FICO's large processing clients has deployed its adaptive analytics technology. The client captures transactions tagged as fraud as well as TC40 customer dispute data and feeds it back into the model's database on a nightly basis. The client says this process does a much better job of keeping models calibrated than the prior approach, which relied on annual model updates.

Clients are also complimentary of the stability of the software, saying they rarely have an issue with bugs or outages. Feedback on the upgrade process is not as glowing; as is often the case with vendors whose software has a heavy client footprint, clients classify the upgrade process as "challenging" and "cumbersome."

In terms of areas needing improvement, some clients (primarily those in the U.K. and Canada) voice a good deal of frustration about the April 2018 Falcon model refresh. This model does not work well for these issuers' CNP fraud, which represents the bulk of payment card fraud in the U.K. and Canada, and many have experienced escalating losses as a result. Another area of improvement that clients would like to see is responsiveness to enhancement requests. Client feedback is that it can take years for client requests to manifest in the production product, so they'd like to see FICO improve upon execution timelines and accelerate the speed of development.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

Table S provides a summary of client feedback on FICO's strengths and improvement opportunities.

Table S: Key Strengths and Improvement Opportunities—FICO

Strengths	Improvement opportunities
Analytics acumen and model performance	Time to market for requested enhancements
Software stability	CNP model performance in the U.K. and Canada after April 2018 model refresh
Embedded risk intervention capabilities	

Source: Aite Group

NICE ACTIMIZE

Nice Actimize is one of the leading providers of financial crime solutions; all of the global top 10 banks and more than 200 FIs around the world use Nice Actimize solutions. The company provides real-time, cross-channel fraud prevention, AML detection, and trading surveillance solutions that address such concerns as payment fraud, cybercrime, sanctions monitoring, market abuse, customer due diligence, employee fraud, and insider trading. Nice Actimize provides enterprise risk management solutions to banks, insurance companies, payment companies, and government entities in 70 countries.

AITE GROUP'S TAKE

Nice Actimize uses several machine learning algorithms in its models, depending on the business need—both supervised (XGBoost, random forest, regression, etc.) and unsupervised (clustering, isolation forest). Nice Actimize delivers machine learning intelligence to its clients in a few manners:

- **Core product deployments**: Every new Nice Actimize customer receives machine learning models in production and ActimizeWatch for cloud-managed optimization. Nice Actimize is in the process of introducing machine learning models into existing customers' implementations as well. One method of doing this is to combine existing expert-designed models with machine-discovered features, using the ActimizeWatch environment to alter model parameters rapidly. This approach allows its customers to continue use of existing models while introducing machine learning for agility and nuance to handle new fraud patterns.
- **ActimizeWatch**: ActimizeWatch was built to face the growing challenge of rapid changes in fraud patterns as well as FIs' more frequent release of new payment products, which dictate the need for agile analytics optimization. ActimizeWatch tackles the problem by providing a cross-institution view of data and threats, and using this intelligence to optimize analytics. ActimizeWatch monitors analytics performance and transactional data in the cloud across multiple organizations, using machine learning to discover patterns that affect a wide range of institutions.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

ActimizeWatch puts this intelligence to work by optimizing each FI's analytics using the risk variables and patterns found across the market.

- **Custom-developed models:** Nice Actimize's data scientists partner with clients to build analytic models relying on a library of several hundred predictive risk features. These risk features were developed in the field on broad customer data to solve a wide array of common and complex fraud scenarios.

In-market use cases using Nice Actimize's machine learning modeling capabilities include card fraud, remote channel fraud, and AML.

BASIC FIRM AND PRODUCT INFORMATION

- **Headquarters**: New York
- **Founded:** 1999
- **Number of employees**: 1,150
- **Ownership**: NICE (Nasdaq: NICE)
- **Percentage of revenue invested in R&D:** More than 15%
- **Product names:** Actimize Integrated Fraud Management (IFM) platform and Autonomous AML
- **Target customer base:** Financial institutions, issuing processors, and fintech firms
- **Implementation options:** On premises, private cloud, or public cloud (AWS)
- **Average new machine learning client wins per year over the past three years:** Undisclosed
- **Next release date**: IFM-X (June 2019); Autonomous AML, CDD (2019)

TOP THREE STRATEGIC PRODUCT INITIATIVES COMPLETED IN THE PAST 12 MONTHS

- **Automation of machine learning modeling and execution:** Throughout 2018 Nice Actimize operationalized and automated ActimizeWatch, its managed analytics service. As part of the ActimizeWatch service, Nice Actimize prepares data for analytics development and optimization, porting it from the production environment onto a cloud-based analytics modeling environment, and then porting back analytical models from the cloud into the production environment. Over the last year, Actimize onboarded more than 20 FIs onto ActimizeWatch, fueling its collective intelligence, based on a market-wide view of fraud typologies.
- **Customer-authorized fraud models:** Nice Actimize built solutions that detect customer-authorized fraud (such as business email compromise), scams, and different techniques involving social engineering. Using a combination of expert

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

features and ML-discovered features, Nice Actimize built new models that have proven effective at detecting such fraud scenarios.

- **Faster payments models:** Nice Actimize has expanded its payments fraud solutions, specifically catering for Zelle and The Clearing House RTP payments. These include profiling incoming funds into accounts, considering the risk of "request to pay" features, etc.

TOP THREE STRATEGIC PRODUCT INITIATIVES IN THE NEXT 12 TO 18 MONTHS

As part of its journey to autonomous financial crime management, which includes analytics and automation in every step and is materialized in the X-Sight platform-as-a-service solution, Nice Actimize is heavily investing in the following:

- **Fraud hub platform:** Substantial technology improvements will be applied to the product and aimed to improve detection performance, simplify integration into the client's ecosystem, reduce total cost of ownership, improve latency and throughput, and make the product more flexible and agile. The majority of this will involve utilization of big-data technologies, new integration technologies, and a new AI execution engine.
- **Analytics agility:** Nice Actimize is planning to extensively invest in empowering customers to self-sufficiently manage their own risk models, enabling them to respond quickly to changes in data (such as new products or new fraud patterns). The product will provide a set of tools and capabilities that customers' data scientists can leverage to manage an end-to-end modeling cycle. This includes obtaining the data required from model discovery and feature engineering, simulation, and testing of the models; automated model training; and deploying the new/updated models in production quickly and safely, while leveraging a patent-pending model explainability capability for white-boxing machine learning models to support model governance.
- **Automation in fraud operations:** Automation of activities taken by the alert investigators combined with automated data-driven decisions and even completely auto-resolving alerts will dramatically reduce the alert resolution time and overall operational cost. Nice Actimize's focus areas include a substantial investment in providing automated actions and workflows, predefined by the product, and enabling investigators to define their own custom automated steps based on their own specific requirements, as well as integrating AI to improve and automate key decision points, such as alerts, workload distribution, and alert disposition.

CLIENT FEEDBACK

Nice Actimize's client references give the firm high marks for the analytical performance of its machine learning models as well as the responsiveness and partnership of its professional services and client support teams. After a custom model development process, one of Nice Actimize's customers is now at a 34% detection rate for its most painful card fraud vector, while its in-market peer banks using other solutions are averaging an 8% detection rate. Another client

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

says that although it took longer than he would've liked to receive the models (12 months from start to finish, six months of which was due to the bank's internal efforts to corral the requisite data), the models Nice Actimize produced are good. IFM's UI is another area that receives high marks from client references.

In terms of improvement opportunities, one point of frustration mentioned is the fact that machine learning modeling is not an integral part of the platform as it is with some of Nice Actimize's competitors. As a result, the model development process takes longer, and the output is a black-box model that requires Nice Actimize's involvement for creation, tweaks, and retraining. The scalability of the solution was also mentioned as an area needing improvement—when the customer has a high volume of transactions to sort through and analyze, meeting the SLA can be a challenge.

Many of the above-mentioned challenges have been addressed with some of Nice Actimize's newer offerings. ActimizeWatch enables the citizen data scientists to build and deploy their own models, while IFM-X is built natively on big-data technologies such as Cassandra and Hadoop, which improves scalability. The disconnect between the experience of the installed customer base that is on older versions of legacy technology and a vendor's latest offerings are not unusual in a market that is rapidly transitioning to the next generation of technology.

Table T provides a summary of feedback on Nice Actimize's strengths and improvement opportunities.

Table T: Key Strengths and Improvement Opportunities—Nice Actimize

Strengths	Improvement opportunities
Model performance	Scalability
Service and support responsiveness	Cohesion with core platform
User interface	

Source: Aite Group

RISK IDENT

Wholly owned by German retail giant Otto Group, Risk Ident offers antifraud solutions to companies within the e-commerce, telecommunication, and financial services sectors. Risk Ident helps firms reduce cross-channel ATO, payment fraud, and account and loan application fraud leveraging its domain knowledge and machine learning technology.

AITE GROUP'S TAKE

Risk Ident's machine learning technology employs a combination of techniques—including naive Bayes, decision-tree ensembles, and association rules mining—and combines these with graph database technology to facilitate rapid detection of anomalous behavior and suspicious linkages. In-market fraud use cases include merchant CNP fraud, ATO, and new-account fraud.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

The modeling capabilities are fully developed and maintained by Risk Ident. While the company's primary focus is the European merchant and telecom markets, it also has a handful of FI use cases in production.

Risk Ident also offers native device analysis and recognition capabilities, which includes consortium-based device reputation intelligence. This data serves as a valuable additional input into Risk Ident's machine learning fraud scoring.

BASIC FIRM AND PRODUCT INFORMATION

- **Headquarters**: Hamburg, Germany
- **Founded:** 2012
- **Number of employees**: 78
- **Ownership**: Otto Group
- **Percentage of revenue invested in R&D:** More than 15%
- **Product names:** Frida One, Frida ML, and Device Ident
- **Target customer base**: European e-commerce merchants, telecom, and financial services firms
- **Modeling:**
  - **Citizen-data-scientist enablement?** No
  - **Vendor-developed and maintained models?** Yes
  - **Support for import of external models?** No
- **Implementation options**: On premises, private cloud, or vendor-hosted
- **Average new machine learning client wins per year over the past three years:** Seven
- **Next release date**: Minor release in March 2019, new version in summer 2019

TOP THREE STRATEGIC PRODUCT INITIATIVES COMPLETED IN THE PAST 12 MONTHS

- Re-architecture to enhance scalability
- Streamlined model training and evaluation workflow
- Multiclass prediction for automatic discrimination of fraud types

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

TOP THREE STRATEGIC PRODUCT INITIATIVES IN THE NEXT 12 TO 18 MONTHS

- Adaptive UI using machine learning to always provide the user with the most relevant information in the current context for improved usability and efficiency during manual review
- Automatic analysis and interactive exploration of large fraud graphs for detecting, visualizing, and handling known suspicious and anomalous structures
- Prebuilt integrations with market-specific external data sources, with intelligent source selection

SAS

A longstanding leader of risk analytics, SAS was founded in 1976 and remains privately held. With US$3.2 billion in revenue in 2017, SAS serves FIs, corporations, and government entities in 145 countries. SAS' financial crimes solutions use advanced data analytics to monitor payments, nonmonetary transactions, and events, enabling businesses to identify and respond to unwanted and suspicious behavior in real time.

AITE GROUP'S TAKE

SAS enables machine learning through supervised and unsupervised models using multiple techniques, including neural networks, deep learning, gradient boosting, random forest, logistic regression, clustering, and Bayesian. The firm enables deployment of machine learning models within its platform solutions in the following ways:

- **Native model-building capability:** SAS' adaptive learning capability enables clients' data scientists or data analysts to build custom machine learning models themselves. The solution provides a suite of solutions that help with feature identification and creation of machine learning models using a variety of algorithms (e.g., logistic regression, random forests, gradient boost, neural networks), then facilitates side-by-side comparisons of model performance using the client's historical data. Once the client has identified the optimal model configuration, the model can be deployed into the SAS Fraud Management platform using PMML.
- **Import third-party models:** SAS can support the import of third-party or bank-developed models via PMML.
- **Core product deployment:** SAS' Fraud Management platform employs neural network models that have self-learning capabilities. This also supports multitenant deployment with customization available at the subtenant level.

Some of SAS's clients are still on older on-premises versions that can't benefit from some of its more advanced adaptive learning options and are reliant on annual model refreshes. SAS' latest release includes migration routines to help make the transition from the more rigid data structures to the more adaptive data management approach less of a rip-and-replace experience. SAS is also doing some hybrid installs combining on-premises and cloud versions to

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

help with the migration from the older solutions to the newer, more adaptive platforms. SAS' long-term product strategy is to move away from relational databases altogether and toward a more flexible, streaming big-data approach.

In-market use cases for SAS' machine learning models include debit card, real-time payments, and SWIFT fraud risk assessment.

BASIC FIRM AND PRODUCT INFORMATION

- **Headquarters**: Cary, North Carolina
- **Launched in:** 1976
- **Number of employees**: 14,151
- **Ownership**: Wholly owned by co-founders James Goodnight and John Sall
- **Percentage of revenue invested in R&D:** 26%
- **Product names:** SAS Fraud Management, SAS Detection and Investigation, and SAS Visual Investigator
- **Target customer base**: Financial institutions, issuing processors, acquiring processors, and merchants
- **Modeling:**
  - **Citizen-data-scientist enablement?** Yes
  - **Vendor-developed and maintained models?** Yes
  - **Support for import of external models?** Yes
- **Implementation options**: On premises, private cloud, vendor-hosted, or public cloud (AWS, Azure, Google)
- **Average new machine learning client wins per year over the past three years:** 75
- **Next release date**: June 2019

TOP THREE STRATEGIC PRODUCT INITIATIVES COMPLETED IN THE PAST 12 MONTHS

- Visual-based data exploration and guided rule writing development
- Flexible messaging layouts to support the ongoing need for additional and varied third-party data (data integration adapters)
- Additional integration of adaptive and self-learning analytics to assist with false-positive reduction and identification of new financial crime activities

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

TOP THREE STRATEGIC PRODUCT INITIATIVES IN THE NEXT 12 TO 18 MONTHS

- Client-developed and client-deployed machine learning modeling
- Single platform for transaction and identity fraud
- Customer insight platform

CLIENT FEEDBACK

SAS brings a strong reputation for advanced analytics, and client references are complimentary of the strength of the management team as well as SAS' reputation in the market. SAS also receives high marks for delivering high-performance models with low latency (30 to 40 milliseconds for debit card risk assessment). The operations team is commended for its strong execution in terms of project management as well as service and support.

The following are key areas of improvement/enhancement that SAS' clients would like to see:

- **Quicker model development process:** In the words of one executive interviewed, "The current time frame of six months to prepare new models, combined with the bank's deployment cycle, is just too long given the pace with which fraud patterns change."
- **Eight-eye approval:** Clients would like more flexibility in regard to the levels of approval to deploy new rules.
- **Third-party integrations:** Clients would like to see more default integrations with a range of fraud/cyber providers to further enrich the solution's analytics.

Table U provides a summary of client feedback on SAS' strengths and improvement opportunities.

Table U: Key Strengths and Improvement Opportunities—SAS

Strengths	Improvement opportunities
Model performance and response time	Third-party integrations
Client service and support	Shorter model refresh/creation time frames

Source: Aite Group

SIMILITY

Simility, a PayPal service, helps businesses orchestrate decisions to reduce friction, improve trust, and solve complex fraud problems by combining machine learning and big-data analytics. Simility's offerings are underpinned by its Adaptive Decisioning Platform, built with a data-first approach to help businesses harness their data and better assess transactional risk. Simility's analytics help merchants, FIs, and processors reduce friction, improve trust, and solve complex fraud problems.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

AITE GROUP'S TAKE

Founded by former Google executives responsible for its fraud-fighting efforts, Simility's starting point logically was in the digital environment. The firm has a strong competency in merging digital inputs with advanced data analytics. The capabilities extend beyond digital, however, into the omnichannel environment. Simility brings clients a platform they can use to develop and deploy custom machine learning models and also offers native capabilities within its platform to identify and capture valuable inputs, such as device fingerprint and behavioral biometrics. Simility's customers have deployed its machine learning model-building capabilities across a variety of use cases, including check fraud, application fraud, and both retail and wholesale banking ATO.

One of Simility's key strengths (as could be anticipated, given the Google roots) is in the platform's ability to incorporate, manage, and analyze data from a variety of disparate inputs. Simility customers benefit from a comprehensive data lake of enterprise and third-party data that is created as part of the standard implementation process, which is then enriched to provide optimal financial crime mitigation capabilities. This data lake is automatically created by Simility administrators as they add data feeds and configure machine learning models without tapping into the client's IT or engineering resources.

BASIC FIRM AND PRODUCT INFORMATION

- **Headquarters**: San Jose, California
- **Launched in:** 2014
- **Number of employees**: 80
- **Ownership**: Wholly owned by PayPal
- **Percentage of revenue invested in R&D:** More than 15%
- **Product name:** Enterprise Fraud Management Platform (EFMP)
- **Target customer base**: Merchants, FIs, fintech firms, and processors
- **Modeling:**
  - **Citizen-data-scientist enablement?** Yes
  - **Vendor-developed and maintained models?** Yes
  - **Support for import of external models?** Yes
- **Implementation options**: On premises, private cloud, or public cloud (AWS and Google)
- **Average new machine learning client wins per year over the past three years:** 15
- **Next release date**: April 2019

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

TOP THREE STRATEGIC PRODUCT INITIATIVES COMPLETED IN THE PAST 12 MONTHS

- **Create pre-trained, out-of-the-box models for ATO, account origination, and transaction fraud:** This offering uses network learnings and historical performance across the customer base to create a turnkey approach for quick deployment. The initial deployment is based on preset rules, and the model quickly evolves based on real-time data and actual transactions using rule tuning and the ability to run multiple challenger models. This provides mid-market customers with the ability to use state-of-the-art, big data-based machine learning models without the extensive investment of hiring data scientists.

- **Machine learning enhancements:** The platform generates machine learning models automatically based on the input data and fraud-prevention goal. It provides a comparison of models and allows the deployment of the selected model (retraining and tuning the model without any feature engineering to find a better-fitting model). This also includes feature engineering, hyper-parameter turning, feature selection (to enhance, delete or add features), model selection (neural-net, linear models, ensemble, tree-based model), and finally model ranking to find the most accurate model. Instead of being a black box, machine learning explainability allows analysts to see features selected by the model and understand their significance, leading to a final model score.

- **Platform enhancements:**

    - Historical data modeling (back-testing of strategies and model): This enables the testing of rules with historical data, analyzes the historical performance of rules, and allows the testing of auto-decisions with historical data.
    - Champion challenger and rule-tuning: This enables fraud analysts to change parameter values and test the performance of rules to compare the impact of rule changes before implementing them in the live environment. Simility enables ongoing rule-tuning using historical performance analysis with performance visualization and recommended changes.
    - Maker checker: This separates rule-creator and rule-approver duties, preventing unintended errors prior to activating new rules.

TOP THREE STRATEGIC PRODUCT INITIATIVES IN THE NEXT 12 TO 18 MONTHS

- **Machine learning enhancements:** These include automated feature generation to help data scientists automatically create features from a data set; an auto encoder, which is a neural-network-based unsupervised learning methodology for dimensionality reduction and anomaly detection; and capabilities to standardize model predictions (abstracting the process of deploying the model to provide a consistent interface regardless of the platform of choice of the data scientist). This will enable rapid deployment for the data science decisions teams, leading to fast response time by accelerating the time to market.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

- **Integration into PayPal and Braintree:** Simility will be powering the fraud solution component of the PayPal and Braintree offerings and will be able to leverage PayPal network intelligence in real time in the Simility models.
- **AML and fraud models:** Simility will be deploying models to solve for the evolving financial crime space (and to meet regulations). These include models for authorized push payments in the U.K. and a preconfigured AML data model, with rules and decisions that include Know Your Customer (KYC) checks, watch-list matching, sanction screening, and advanced analytics.

CLIENT FEEDBACK

Simility receives high marks from the clients interviewed, which include banks and e-commerce firms, for its service and support as well as the product features. Clients are complimentary of the overall flexibility of the platform across a variety of financial crime use cases, as well as EFMP's ability to bring data from multiple internal and external sources into the models. Simility's responsiveness and collaborative approach to meeting its clients' needs are also highlighted; one of its clients says that Simility is a true partner, not just a vendor. Another of Simility's FI clients is also complimentary of Simility's device identification capabilities, saying that the system does well in recognizing the same device over time, which can be a challenge in the browser-based environment.

Implementation time frames were surprisingly quick. A neobank implemented Simility's cloud solution within 30 days, while a large regional bank implemented the on-premises solution in six months (and acknowledged that the vast majority of the elapsed time was due to delays on the bank's side).

Simility employs a state-of-the-art tech stack, and one FI interviewee acknowledges that the technology was initially a bit intimidating to the FI's IT team. The FI client reference that implemented the EFMP solution on premises says that migrating to more modern technology was ultimately good for the FI. The interviewee says that the Kafka and Cassandra required to support Simility turned out to be easier to work with than its previous homegrown technology.

In terms of areas needing improvement, EFMP's UI receives tepid marks from the client references, and a couple of them highlight it as an area in which they would like to see improvement—improvements to look and feel as well as workflow to make it more user-friendly, more flexibility, and enhancements to make it easier to partition specific work groups are all wish-list items. Table V provides a summary of client feedback on Simility's strengths and improvement opportunities.

Table V: Key Strengths and Improvement Opportunities—Simility

Strengths	Areas of improvement
Collaborative approach to implementation and support	User interface
Embedded device identity capability	
Data handling	

Source: Aite Group

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

THETARAY

ThetaRay is dedicated to helping clients at large financial organizations become more resilient and seize opportunities. Its unsupervised machine learning solutions are designed to help clients manage risk, detect money laundering schemes, uncover fraud, expose bad loans, uncover operational issues, and reveal new growth opportunities.

AITE GROUP'S TAKE

ThetaRay applies unsupervised machine learning algorithms to multidimensional data using proprietary dimension-reduction algorithms. ThetaRay's offering is somewhat different from many of the other vendors in this AIM evaluation, given the platform's strong reliance on unsupervised analytics. Rather than putting model-building tools in the hands of the FI's citizen data scientists, ThetaRay applies unsupervised analytics to its clients' data sets.

Unsupervised analytics are a double-edged sword for vendors focused on financial crime. They are quite beneficial from an AML performance perspective given the relative lack of training data to inform detection models. The benefits of applying unsupervised analytics to AML are manifested in the high praise for the system's performance from ThetaRay's clients. However, many regulators still have a heavy emphasis on transparent model performance, and there is a perception among regulators that this is harder to achieve with unsupervised techniques.

BASIC FIRM AND PRODUCT INFORMATION

- **Headquarters**: Hod HaSharon, Israel
- **Launched in:** 2013
- **Number of employees**: 100
- **Ownership**: Jerusalem Venture Partners and angel investors
- **Percentage of revenue invested in R&D:** More than 15%
- **Product name:** ThetaRay Analytics Platform
- **Target customer base**: FIs and insurance companies
- **Implementation options**: On premises, private cloud, public cloud, or supporting clients on AWS, Azure, and GCP
- **Modeling:**
  - **Citizen-data-scientist enablement?** No
  - **Vendor-developed and maintained models?** Yes
  - **Support for import of external models?** No
- **Average new machine learning client wins per year over the past three years:** More than 10
- **Next release date**: Q2 2019

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

TOP THREE STRATEGIC PRODUCT INITIATIVES COMPLETED IN THE PAST 12 MONTHS

- Creating an investigation center—an optional workflow, case management, and forensic data analysis tool for financial services firms that wish to deploy a new front end for analysts rather than augmenting existing tools
- Automating data drift recognition, adjusting normality as products, usage patterns, and customer base shift in a transparent, interpretable manner
- Increasing the horizontal scalability of core analytic algorithms across more Hadoop nodes, leveraging inherent parallelism built in to the core technology for ever larger deployments

TOP THREE STRATEGIC PRODUCT INITIATIVES IN THE NEXT 12 TO 18 MONTHS

- It plans to make continuous analytics investments toward increasing explainable results, additional algorithms targeting risks and increasing detection performance, productization of newer data sources, such as blockchain data, and further reduction of analytic latency in streaming applications.
- It plans to implement multientity support within a multijurisdictional FI for securely isolated legal entities that wish to deploy more efficiently in a single-scalable solution, balancing consolidation and a singular customer view with strict data privacy and segregated operational compliance requirements.
- Solution APIs are a focus for simplifying delivery into existing enterprise financial crime solutions, including data management, KYC, and regulatory filing. The goal is to enable clients faster time to value within their overall financial crime strategy and to enable partner tools for scalable delivery success.

CLIENT FEEDBACK

ThetaRay's reference clients include two large European FIs and one large Asian bank. One is in a POC, another has moved from POC to pilot, and the third is in production with ThetaRay for AML transaction monitoring use cases. Thus far, the results are impressive for the banks interviewed. One bank has seen a 25% improvement in its false-positive rates for retail and corporate customer transaction monitoring. Another says that when compared to its incumbent scenario-based vendor, ThetaRay detects anomalies much more quickly.

ThetaRay's UI is cited as a strength by one of the interviewees, while another is complimentary of ThetaRay's responsiveness to customization requests—the bank sees ThetaRay as a true partner, not just a vendor. Two of the banks interviewed note that they are pleased that the team that they started working with at the project outset in 2016 has remained intact throughout the duration of the relationship—something that is somewhat unusual in this highly competitive market.

The biggest challenge cited by interviewees is the system's reliance on unsupervised techniques (they also acknowledge that in AML, with the relative lack of training data compared to fraud,

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

unsupervised modeling is an important tool). While the Asian bank's regulator is comfortable with ThetaRay's approach, one of the European banks that is still in the POC stage hasn't shared the concept with its regulator yet. In this executive's words, "Our regulator is not the most innovative and struggles to understand advanced analytics." This bank plans to keep its legacy platform running in parallel with ThetaRay for nine to 12 months and will then present the regulator with side-by-side results in the hope that these results will convince the regulator that ThetaRay's approach is superior.

In terms of wish-list items for the product roadmap, one bank says it would like to see a hybrid solution with more scenarios and supervised capabilities to better address regulators' demand for more transparent AML platforms. Another says that while ThetaRay's detection algorithms are excellent, the bank's requirements for an AML platform are broader than just detection; it's also important to have robust alert and case management, a good graphical link analysis interface, and third-party interfaces via API—it would like to see ThetaRay focus on these in the coming months.

Table W provides a summary of client feedback on ThetaRay's strengths and improvement opportunities.

Table W: Key Strengths and Improvement Opportunities—ThetaRay

Strengths	Improvement opportunities
Willingness to customize	Heavy reliance on unsupervised analytics, with little in the way of supervised options
User interface	
Analytic performance	

Source: Aite Group

THREATMETRIX

ThreatMetrix, a LexisNexis Risk Solutions company, is a leading digital identity firm that delivers the intelligence behind 100 million daily authentication and trust decisions to differentiate legitimate customers from fraudsters in real time. Its solutions provide ThreatMetrix's financial services and merchant clients with real-time insight into 1.4 billion anonymized user identities. ThreatMetrix's Smart Analytics solution enables businesses to deploy custom machine learning models within the ThreatMetrix platform.

AITE GROUP'S TAKE

From a machine learning standpoint, ThreatMetrix is both a producer and consumer of data. Its crowdsourced database's 4 billion devices, 1 billion emails and phone numbers, and hundreds of billions of events are data points that ThreatMetrix brings into the modeling process. ThreatMetrix's platforms support custom models created by the client's data scientists and imported via PMML, or the models can be created by ThreatMetrix's professional services team. In-market use cases for custom machine learning models include social engineering, ATO, and mule detection.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

For those models created by ThreatMetrix, the process begins with automated feature generation. This leverages customer-provided truth data and the ThreatMetrix Digital Identity Network to produce the most significant variables to be used in the model. ThreatMetrix then produces the model, optimizing the performance to produce the smallest number of false positives. The model can be retrained based on new transactions to further improve the performance. ThreatMetrix has productized this approach for general use, and the process can be completed in approximately 30 minutes. The external dependency is the normalization of the truth data. ThreatMetrix's custom modeling approach does not enable the models to be built within the platform itself. ThreatMetrix's custom models largely employ supervised logistic regression techniques, since explainability of outcomes is a priority for the large banks that consume the models.

BASIC FIRM AND PRODUCT INFORMATION

- **Headquarters**: San Jose, California
- **Launched in:** 2005
- **Number of employees**: 278
- **Ownership**: Wholly owned by LexisNexis Risk Solutions
- **Percentage of revenue invested in R&D:** More than 15%
- **Product name:** Smart Analytics
- **Target customer base**: FIs, merchants, and processors
- **Implementation options**: ThreatMetrix's services are available only as SaaS.
- **Modeling approach:**
  - **Citizen data scientist?** No
  - **Vendor-developed and maintained?** Yes
  - **Import external models?** Yes
- **Average new machine learning client wins per year over the past three years:** Seven
- **Next release date**: March 2019

TOP THREE STRATEGIC PRODUCT INITIATIVES COMPLETED IN THE PAST 12 MONTHS

- **Strong model governance and assurance capabilities:** It provides customers with rule, model, and access assurance capabilities that give them confidence in the integrity of the model development cycle. Policy approval and champion/challenger functionality ensure that there are no single points of development reliance or weakness—a clear audit trail of changes and the ability to demonstrate the performance implications of any changes before putting them into production.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

Additionally, single sign-on capabilities allow customers to manage their own user access protocols and permissions, further improving the integrity of provisioning customer portal access.

- **ThreatMetrix ID Trust Score and rules:** Leveraging the development of the ThreatMetrix ID and the creation of a unified digital identity, ThreatMetrix ID Trust Score provides a network view on the integrity and trust in that digital identity. Based upon feedback and performance data from across the ThreatMetrix Digital Identity Network, this machine-learning-based trust score enables customers to reference the performance of a digital identity across the network and interpret the risk associated with that performance in its own strategies.
- **Integration of LexisNexis Risk Solutions' identity assurance solutions:** ThreatMetrix has created the opportunity for customers to directly integrate with identification and authentication solutions from LexisNexis Risk Solutions, including Email Risk Assessment, Phone Finder, Order Score, InstantID, and FraudPoint. Dynamically referencing the data, risk score, and profiles from those solutions, ThreatMetrix is enhancing the decision-making process, integrating physical and digital identity risk assurance capabilities, and providing an end-to-end customer-decision capability.

TOP THREE STRATEGIC PRODUCT INITIATIVES IN THE NEXT 12 TO 18 MONTHS

- **Enhanced machine learning capabilities for customers:** This will empower customers to build their own smart-learning models directly into the ThreatMetrix solution without the need for ThreatMetrix Professional Services support—providing customers with direct control of policy management and optimization. And by leveraging the performance data of customers for the benefit of customers, ThreatMetrix will continue to develop and implement more flagship machine learning models. By providing optimized industry, geography, and user case fraud models that can supplement or replace a customer's own models, ThreatMetrix will continue to optimize the strength of the network to empower better decisions.
- **Leverage customer data through consortium data sharing:** It will provide the opportunity for customers to develop their own consortium networks and enable trusted peers to share data that focuses on shared problems and shared risks.
- **Extended data model:** It will implement a two-party payment data model, offline and batch-data ingestion bridger watch-list integration, and a UI that better enables fraud and financial crime decisions and investigations. Extension of the ThreatMetrix data model will increase the breadth, depth, and scope of customer decisions. Batch data and process enrichment will enable customers to better integrate their internal business processes with ThreatMetrix, ensure that risks can be better identified, and break down some of the challenges that exist between fraud and financial crime.

CLIENT FEEDBACK

One of ThreatMetrix's key strengths is the level of service and support it provides to its clients. This vendor consistently gets high scores from clients for its service and support, and for its

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

responsiveness to requests for enhancements. As an example, the genesis of its custom machine learning modeling capability was actually a client request—ThreatMetrix added its custom modeling component at the request of a large banking client and partnered with that client on requirements development to ensure the solution met the business need. A couple of the ThreatMetrix clients interviewed voice a bit of trepidation over the LexisNexis Risk Solutions acquisition. They are worried that the firm's level of responsiveness will be impacted once the nimble startup is subsumed within a much larger organization, though they say thus far they've seen no noticeable impact.

Another point of strength for ThreatMetrix is a bit of a double-edged sword. ThreatMetrix's roots are in the digital identity space—it analyzes billions of banking and e-commerce transactions per year to assess the risk of the device and the associated persona. As a result, it brings a wealth of consortia-based data that can feed the models, which can be further augmented with its clients' internal and external data sources.

These roots are unique relative to the other firms in this vendor evaluation, for which the data analytics platform was their starting point. As a result of this path, the ThreatMetrix custom machine learning modeling capability is a bit less evolved from a feature/functionality perspective than some of its competitors. Some basic elements, such as a sandbox to test new models against historical data and the ability to ingest and analyze unstructured data, are still missing, and one of the large bank clients interviewed expresses the belief that ThreatMetrix's team is still a bit too lean and green when it comes to building custom machine learning models—for this reason the bank is having its own data scientists do all of the custom model development.

Table X provides a summary of client feedback on ThreatMetrix's strengths and improvement opportunities.

Table X: Key Strengths and Improvement Opportunities—ThreatMetrix

Strengths	Improvement opportunities
Strong digital identity solution	Further build internal data analytics competency
Responsiveness to client requests	Needs a sandbox environment for model testing

Source: Aite Group

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

CONCLUSION

Fraud and AML machine learning platforms are an active area of investment as businesses look to the next generation of technology that can help combat financial crime while maintaining positive customer experiences. Here are a few recommendations for both buyers and vendors in this rapidly evolving space:

Buyers:

- **Clearly define your current and future needs.** Map out both near- and long-term use cases for the platform. Ensure you also have a clear picture of your firm's strengths and limitations. Do you have a strong existing data science team that will primarily want to build and maintain its own models, or does your firm need a vendor that can take on the majority of the model development and maintenance?
- **Understand how the vendors' offerings map to these needs.** While the marketing messages of many of the vendors in the space may sound similar on the surface, the strengths and weaknesses are quite different once you dig into the capabilities at a more granular level. A solid internal needs assessment as part of the business case process will help guide the selection of the appropriate vendor.
- **Make sure data ingestion is a well-defined part of the plan.** A solution's output is only as good as the data inputs, and harnessing internal data to feed the solution is often one of the most challenging aspects of a platform integration project. Perform a mapping of what data is available and when (e.g., can it be streamed in real time, or is it only available in batch?). Also, plan for data standardization and cleansing as part of the platform implementation, and budget for those resources, whether they are internal or tap into the vendor's professional services team.
- **Consider the cloud.** The cloud can help significantly reduce the total cost of ownership on an ongoing basis and also enable access to the vendor's latest and greatest product release on a timely basis. As a result, many FIs interviewed for this report are taking significant portions of their fraud and AML detection to the cloud.

Vendors:

- **Continue to invest in R&D.** This market is progressing rapidly, driven by stiff competition and the escalating threat environment. Only those firms with a strong commitment to product innovation will maintain market relevance.
- **Ensure the solution's output is transparent and explainable.** Even though regulators are (finally) signaling more openness toward the use of advanced analytics for financial crime detection, the reality is that the wheels of progress tend to move slowly in highly regulated environments. The expectation that analytic outcomes are explainable will likely be a market reality for some time to come.
- **Make sure you can support your success.** Rapid growth can be a double-edged sword. Ensure that your service and support function provides excellent and responsive support—word travels fast for those vendors that trip up in this regard.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

RELATED AITE GROUP RESEARCH

AIM Evaluation: Identity Document Capture and Verification, October 2018.

The AML of Tomorrow: Here Today, July 2018.

Synthetic Identity Fraud: The Elephant in the Room, May 2018.

Machine Learning: Fraud Is Now a Competitive Issue, October 2017.

Machine Learning for Fraud Mitigation: The Substance Behind the Buzz, April 2017.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

ABOUT AITE GROUP

Aite Group is a global research and advisory firm delivering comprehensive, actionable advice on business, technology, and regulatory issues and their impact on the financial services industry. With expertise in banking, payments, insurance, wealth management, and the capital markets, we guide financial institutions, technology providers, and consulting firms worldwide. We partner with our clients, revealing their blind spots and delivering insights to make their businesses smarter and stronger. Visit us on the web and connect with us on Twitter and LinkedIn.

AUTHOR INFORMATION

Julie Conroy
+1.617.398.5045
jconroy@aitegroup.com

CONTACT

For more information on research and consulting services, please contact:

Aite Group Sales
+1.617.338.6050
sales@aitegroup.com

For all press and conference inquiries, please contact:

Aite Group PR
+1.617.398.5048
pr@aitegroup.com

For all other inquiries, please contact:

info@aitegroup.com

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com