CELENT

XCELENT Awards 2018

SOLUTIONS FOR ANTI-MONEY LAUNDERING

2018 TRANSACTION MONITORING ABCD VENDOR VIEW

Neil Katkov, PhD
September 2018

OLIVER WYMAN

CONTENTS

INTRODUCTION

Anti-money laundering software solutions are crucial supports for AML compliance at financial institutions and other firms involved in funds transfer and value exchange. At the same time, rising compliance costs, intractable operational bottlenecks, the burden of false positives, and other operational trends are posing distinct challenges to both financial institutions and the AML software systems on which their compliance operations depend.

Emerging technology such as artificial intelligence (AI) and robotic process automation (RPA) holds significant promise for overcoming some of these issues. At the same time, a new wave of regtech challengers is moving quickly to deploy such next-generation technologies and is emerging as competition to incumbent AML software providers. In response, AML software providers are building out new capabilities of their own leveraging advanced technologies.

Such is the environment surrounding this, Celent's fourth review of AML transaction monitoring software systems available to financial institutions (a companion report evaluates providers of watchlist screening software). Despite dramatic growth in AML technology and operations spending, the continual emergence of new players, and the potential challenge posed by regtech, the roster of leading AML software providers profiled in this report is largely unchanged since Celent's last edition.

The durability of AML software is perhaps due to the prolonged investment of expertise, energy, and cost — not to mention blood, sweat, and tears — by financial institutions, compliance experts, software technology providers, and regulators. This has resulted in a highly specialized compliance regime with complex requirements for governance, model risk management, and accountability. AML software providers were there at the creation and, as part and parcel of these developments, have accumulated the capabilities, experience, market share, and regulatory trust needed to compete in the rapidly changing AML compliance space.

AML software continues to evolve. Solution providers have been responding to demands for new functionality driven by financial institutions and regulators alike. Some changes have been architectural, such as porting of solutions to more agile, .NET/Java-based platforms; upgrading user interfaces to modern browser technology such as HTML5; providing support for web services and API integration; boosting scalability and performance; and supporting cloud deployment.

More vendors have introduced false positives reduction techniques, alert roll-ups, and other features to support increased efficiency at the alert investigation and case management level. Solutions have also received essential enhancements such as historical profiling, entity-based AML analysis (holistic AML), and real-time analysis.

Importantly, AML software providers are now developing new capabilities leveraging next-generation technologies. These new capabilities, catalogued in this report, include parameter and scenario optimization based on advanced analytics and machine learning (a requirement driven by regulators in especially the US, UK, and Australia); auto-alert closing using machine learning and robotic process automation (RPA); AI-driven transaction monitoring; unstructured data analysis; and natural language generation.

AML SOLUTIONS: DEFINITION AND FUNCTIONALITY

Key Research Question

1

What is an AML transaction monitoring system?

Anti-money laundering systems underpin AML compliance operations at financial services firms and other companies involved in funds transfer. AML system functionality includes transaction monitoring and watchlist screening, as well as modules supporting case management and reporting processes.

Anti-money laundering systems underpin AML compliance operations at banks, securities and investment firms, insurers, third party payment providers (TPPs), fintechs, money services businesses, casinos, cryptocurrency exchanges, telecoms, and other companies involved in funds or value transfer.

While there is a continuing trend among vendors toward offering a suite of solutions providing end-to-end AML functionality, some vendors focus on a subset of the AML value chain, such as watchlist screening. Similarly, while there is a trend among users to source AML technology from one provider, many financial institutions take a best-of-breed approach and work with multiple vendors for their AML needs.

DEFINITION

AML systems provide functionality for transaction monitoring as well as watchlist screening for payments and wires, onboarding, customer due diligence (CDD), and other know your customer (KYC) processes. These functions may be tightly integrated on a single platform or they may comprise distinct modules with varying degrees of integration.

AML SUITE CAPABILITIES

Celent categorizes anti-money laundering solutions into five suite-level functional categories. These categories correspond to the basic modules offered by many AML software vendors. This report evaluates the transaction monitoring (TM), case management, and reporting capabilities of AML software vendors.

Some vendors offer value-added capabilities via additional modules; examples include business intelligence-based visual reporting, graph analysis, and scenario tuning modules. This report discusses and evaluates such capabilities under the appropriate suite-level category.

A companion report, *Solutions for Watchlist Screening: 2018 ABCD Vendor View*, evaluates watchlist (WL) screening and onboarding/CDD capabilities, as well as related case management and reporting functionality.

Figure 1 displays some of the specific features in each suite-level category used to evaluate AML systems in this report. A color-coded version of the same figure appears in the vendor profiles to indicate each solution's support for these features. Additional characteristics of the systems are presented in tables and discussed in the text.

Figure 1: AML Transaction Monitoring System Key Modules and Features

SUITE CATEGORIES	FEATURES AND FUNCTIONS		
Transaction Monitoring	Real time transaction monitoring	Monitors all transactions	Rules engine
	Historical profiling, account level	Historical profiling, peer group	Rules creation
	Link analysis	Searchable rules repository	Rules simulation
Watchlist Screening	See Celent report, Solutions for Watchlist Screening: 2018 ABCD Vendor View		
Onboarding / Customer Due Diligence			
Case Management	Alert risk scoring	Attachments, documents	Attachments, image, audio, and video files
	Case assignment & queueing	Manual email notifications	Automatic email notifications
	Escalations	Visualization tools	Compliance dashboard
	Supports output from 3rd party TM systems	Integrated fraud/AML case management	
Reporting	Regulatory reporting	Auto-generation of regulatory reports	E-regulatory filing
	Prepackaged management reports	Custom report generation	
	Audit trail, user activity	Audit trail, system modifications	

Source: Celent

Transaction monitoring. Transaction monitoring refers to the periodic or real-time analysis of financial and nonfinancial activity to identify unusual account or customer activity that may indicate financial crimes such as money laundering, fraud, terrorist financing, market abuse, or trade misconduct. TM software typically employs SQL query-based rules, which can be quite complex, to identify unusual transactions or sequences of transactions. The TM engine generates exceptions ("alerts") for activity meeting the

rules criteria; many systems will also assign a risk score to the exception indicating the severity of the activity as well as list the specific rules or parameters that triggered the alert. These results are then fed into a case management system for review by compliance analysts.

Some transaction monitoring software vendors offer versions of their solution for multiple use cases — such as anti-fraud or trade surveillance — in addition to AML. This report focuses specifically on the AML capabilities of the solutions.

Case Management. Case management modules support the review of alerts and the creation and investigation of cases by compliance analysts. Operational needs for increased efficiency and regulatory requirements for sound and demonstrable compliance processes make case management arguably the most crucial module of an AML solution. Case management capabilities that support optimized investigation include configurable, domain-specific workflow; interactive screens with data sorting and drilldown; and visualization tools such as behavior analysis charting and network and flow-of-funds visualization (link analysis).

Case management systems may also run additional rules and analytics on the TM systems' output to increase system efficiency through post-processing (that is, post-TM) techniques such as prioritizing alerts for investigation; automatically closing obvious false positive alerts; and routing alerts to the appropriate compliance analysts based on their workload or expertise.

In some cases, financial institutions do not use the case management module of their TM or WL vendor but choose another vendor's case management system or build their own proprietary system that they feel better supports their organization's workflow, procedures, and other requirements.

Reporting. The reporting functionality of an AML system includes support for regulatory reports, as well as internal reporting for management and audit purposes. Key capabilities for regulatory reporting include preconfigured templates for specific regulatory reports, such as suspicious activity reports (SARs), that are auto-populated with case details; and support for electronic filing of these reports for those jurisdictions with e-filing requirements. Internal reporting provides preconfigured as well as custom reports presenting data on alert volumes, investigation timelines, analyst productivity, and other operational statistics. Internal reporting may be presented as a static report; or in graphic form via a compliance dashboard.

AML solutions may also support third party reporting tools, such as SAP Crystal Reports, particularly for custom reports.

Watchlist screening. Watchlist screening involves matching customers, counterparties, and other related entities against lists of individuals and entities issued by governments or regulatory bodies (official watchlists), entity datasets offered by commercial providers, or open source intelligence. Watchlist screening is involved in every step in the AML value chain, including KYC, CDD, and enhanced due diligence (EDD) checks; periodic customer reviews; and sanctions screening for wires and payments. Customer screening may also be a component of ongoing transaction monitoring. Screening solutions are evaluated in the companion Celent report, *Solutions for Watchlist Screening: 2018 ABCD Vendor View.*

Onboarding / Customer Due Diligence. Onboarding and CDD are essential KYC processes that leverage watchlist screening and risk scoring capabilities to create risk profiles of prospective, new, and existing customers. Customer risk scores may also be accessed by TM engines as a parameter for behavior analysis. The onboarding/CDD

functionality of AML vendors is profiled in the companion Celent report, *Solutions for Watchlist Screening: 2018 ABCD Vendor View*.

KEY FEATURES

Below we highlight some of the specific features and functionality that support best-practice AML operations, grouped by the suite-level functional categories described above. Vendor capabilities may vary for each feature. Financial institutions will want to carefully assess which systems support their specific requirements.

Transaction Monitoring Features

The types of rules and analytics available, and the tools provided to manage these, can differentiate AML TM systems.

Rules. Rules interrogate source databases for financial or nonfinancial transactions meeting specific criteria. Because considerable effort and domain expertise go into creating AML rules, the preconfigured rules provided by TM vendors can add value. Both the number of rules and the specific business areas covered, such as correspondent banking, are relevant.

An important consideration for firms that develop rules inhouse is whether and to what extent the system also supports user-configurable rules and user-configurable thresholds and parameters.

Some AML transaction monitoring solutions allow importation of third party analytics and may support Predictive Model Markup Language (PMML) for this purpose.

Rules testing and simulation. This feature, sometimes provided as a separate module, enables users to test new scenarios or adjustments to existing scenarios against a set of the user's historical data before putting them in production. Some solutions provide a sandbox environment to enable extended simulation and analysis of results and automated publishing of rule changes to the production environment to help streamline the process.

Rules testing is an area where vendors are applying advanced analytics and machine learning to optimize fine tuning and segmentation. For larger institutions with sophisticated model risk management operations, the ability to document adjustments and results is an important consideration.

Rules repository. A searchable rules repository assists users with managing vendor-provided rules as well as modified and user-configured rules; putting rules into and out of production (turning rules "on and off"); and documenting rule sets and changes for internal purposes. A rules repository is another important feature for supporting model risk management and documenting rules and modifications for regulators.

False positives reduction. The large number of false positive alerts typically generated by AML systems creates substantial operational and cost burdens for financial institutions. False positives reduction features are therefore important capabilities in an AML system. AML systems may apply various techniques prior to, during, and after the behavior detection process. False positives reduction techniques include rules and thresholds tuning and segmentation, white lists, alert suppression, alert prioritization, and alert triage.

A number of vendors are applying advanced analytics, machine learning, and software robotics (robotic process automation) to the false positives challenge.

Historical profiling, account level: Profiling involves the aggregation and analysis of an account's past transactions to create a baseline of typical behavior for that account. During the monitoring process, transactions that deviate sufficiently from the account's baseline will be flagged. Some systems can create historical profiles at the customer level to support a holistic view of the customer's activity across their various account and product relationships with the institution.

Historical profiling, peer group. Peer profiling is an extension of historical profiling whereby customer or account transactions are compared to the average behavior of that customer's "peer group." Peer profiling involves creating customer segments based on various criteria, such as occupation type or financial product, and running the historical data analysis across all customers in each segment to derive typical behavior profiles for the segments. Activity by an account that deviates sufficiently from the baseline behavior for that account's customer segment will be flagged.

Link/network analysis. At its most basic, link analysis displays transaction flows between accounts. These links or networks may be displayed in graphic form or as tabular information. The analysis may also show various relationships and commonalities between accounts, such as common account holder, beneficial owner, address, business, external counterparty, or other characteristics.

Some link analysis modules can display large numbers of nodes, support interactive viewing by the user, and provide various other visual elements to support analyst investigation. Link analysis visuals are sometimes based on third party visualization tools that have been customized by the AML vendor.

Case Management Features

The depth and flexibility of workflow and analytic tools, as well as post-processing rules and analytics, are important capabilities in case management.

Workflow. Effective workflow for alert and case investigation is crucial for supporting accurate and efficient AML compliance operations. Depending on the needs of the financial institution, both predefined workflows to support specific use cases (for example, transaction monitoring as well as watchlist screening alerts) and configurable workflow and user-definable screens may be relevant capabilities. Support for alert/case escalation and processing deadlines are also key features for case management systems.

RPA and machine learning are important new techniques offered by some vendors for automating aspects of case management workflow.

Case assignment and queuing support. Automated assignment of alerts and cases to available analysts, including alert/case queuing, can support the efficient management of analyst workloads. Some systems include rules to route alerts to specific departments or to analysts with the appropriate domain expertise. Email notifications to inform analysts and supervisors of awaiting tasks is another capability useful in supporting efficient operations.

Visualization. Data sorting and drilldown capabilities support investigation and, depending on their sophistication, can help obviate the need for external data manipulation tools such as Excel. Visual aids to intuitive investigation may include bar, line, and pie graphs of transactional activity, visualization of links and networks, plug-ins such as embedded Google maps, and links to external data sources.

As vendors add advanced analytics, machine learning, and AI capabilities to their systems, sophisticated tools such as graph analysis visualization are emerging.

Attachments. Most systems provide open text windows for analysts to insert ad hoc notes and the ability to attach text-based documents as well as image, video, or audio files. Support for analyst review of files, documents, and links within the case management user interface can assist with streamlined, single-screen investigation.

Support for output from third party AML systems. The capacity to import alerts from third party transaction monitoring systems may be an important consideration for firms that wish to consolidate output from multiple monitoring systems into one alert/case investigation stream; or that are looking to take a best-of-breed approach to selecting their case management module. Some financial institutions run TM output into another vendor's case management system or an inhouse-built case management system.

Support for integrated AML/fraud. Similarly, some case management systems can support alerts from both AML and fraud systems. Capabilities may range from integrated display of AML and fraud activity at the compliance dashboard (BI) level; workflow support for both AML and fraud use cases; integrated display of AML and fraud alerts for investigation; risk scores specific to AML and fraud; and specialized rules or analytics targeted at the interplay between AML and fraud.

Firms looking to centralize their AML and fraud investigative operations onto one platform or that source AML and fraud systems from the same vendor may be interested in these capabilities. Increased regulatory emphasis on the interrelation between fraud and money laundering may drive more demand for this capability moving forward.

Compliance dashboard. Compliance dashboards provide business intelligence (BI) visualization of risk statistics/exposures (such as the number and type of alerts by business unit or geography) and management information (such as analyst productivity or number of regulatory reports filed) to supervisors and other power users as well as to central compliance functions or executives. Compliance dashboards may provide consolidated analysis of output from multiple behavior detection systems, including AML and fraud systems as well as line-of-business or regional systems.

False positives reduction. Post-processing (post-TM) techniques that may be found in a case management module and are aimed at reducing the false positives workload include alert triage and prioritization, alert suppression, and the use of machine learning and RPA to close obvious false positives.

Reporting Features

Internal and external reporting capabilities can support greater efficiency and accountability in regulatory reporting; and provide crucial performance and risk indicators to compliance operations.

Regulatory reporting. Support for regulatory reporting may include auto-population of report details; preconfigured PDF templates for reports for specific jurisdictions; e-filing support for specific jurisdictions; workflow to govern the reporting process; and report storage, search, and retrieval capability.

Reporting modules typically require analysts to write the narrative sections of regulatory reports. However, unstructured data analysis, AI, and natural language generation are now making it possible to automatically compile and write narrative text for AML regulatory reports.

Audit trail. Although requirements may vary depending on the size and situation of the institution, both a complete record of analyst actions on the one hand and a detailed log of system modifications on the other hand, are important to support best practices in internal employee and IT governance, external audit, and regulatory compliance.

Technology Features

Real-time processing. AML systems, due to their focus on regulatory compliance, have typically been deployed on a batch basis, with monitoring of transactions occurring after the fact. This contrasts with fraud systems, which often run in real time in order to stop fraud as it occurs. The continuing growth of digital financial services, fintech, e-commerce, and faster payments, however, is driving demand for real-time behavior detection for AML in these sectors. The convergence of AML and fraud, as well as regulatory interest, may also be factors in moving AML to a real-time paradigm.

Languages and currency. Support for multiple languages and currencies may be important capabilities for AML system implementations across multiple geographies as well as for international lines of business such as correspondent banking.

Language support may range from localized user screens, to double-byte display of non-Latin source data, to double-byte and multilingual analytic capability. Similarly, multicurrency capabilities may be limited to display and single-currency calculations; or may support multicurrency calculations based on rate tables internal to the system.

Data types. AML transaction monitoring primarily involves analysis of financial and nonfinancial transaction data resident in core systems, customer information files, and other structured data sources. The value of alternative data, such as adverse media, in assessing risk; the relevance of information found in PDF files such as contracts and bills of lading; and new analytic techniques such as cluster analysis are all driving increased interest in unstructured data analysis.

System access and permissions. Support for access roles and permissions is important for AML solutions due to the various role levels and supervisory hierarchies inherent in AML compliance operations; and due to the importance of strict governance surrounding rules creation and deployment, case investigation, and system modification.

The ability to define access at a granular level is important for AML system deployments in more complex settings involving multiple business and compliance units, geographies, or other groupings. Safeguarding against unauthorized meddling with the system is also crucial in the compliance environment.

Next-gen tech. The AML technology space is poised for rapid evolution, with advanced technologies including artificial intelligence, machine learning, robotic process automation, and natural language processing/generation all being deployed in efforts to optimize AML compliance operations. The profiles in this report point out the steps AML solution vendors are taking to incorporate these emerging technologies into their offerings.

REPORT METHOD

Key Research Question 2

Who are the leading AML transaction monitoring system vendors globally?

This report profiles 16 AML transaction monitoring systems and indicates the global footprint of their solutions by region; 13 of these vendors are included in the ABCD Vendor View analysis. While some vendors chose not to participate, this report covers many of the leading solutions.

Celent actively reviews vendor systems in the risk and compliance market. This report profiles 16 AML transaction monitoring systems. Most of these solutions qualified for profiles that include customer references. These solutions are also ranked in the ABCD Vendor View.

Celent's ABCD Vendor View analysis is used to highlight vendors that have attained success selling their systems. In general, in order to have a full profile and be included in the ABCD Vendor View grids, an AML transaction monitoring solution had to have:

- At least one new sale to one new customer within the last 24 months.
- At least three live customers.
- Participation by at least three reference customers.

There are 13 solutions that meet these criteria and are included in the ABCD analysis.

Even if a vendor is not included in the ABCD Vendor View, Celent provides a system profile of solutions that met one or more of the criteria. There are three solutions in this category.

EVALUATION PROCESS

Celent sent a detailed request for information (RFI) to a broad set of AML transaction monitoring vendors. Not all vendors chose to participate. After completing the RFIs, each eligible vendor provided a briefing and demo for Celent concentrating on usability and functionality for everyday users, as well as configurability for IT and system administration users.

Celent also asked the references provided by each vendor to complete a survey to obtain their view of the system's business and technology value.

The RFIs and the reference surveys and interviews provided quantitative and qualitative data, much of which is included in this report. Vendors had an opportunity to review their profiles for factual accuracy and to provide their own perspectives, but were not permitted to influence the evaluation. Some of the vendors profiled in this report are Celent clients and some are not. No preference was given to Celent clients for either inclusion in the report or in the subsequent evaluations. Vendors with full profiles are ranked in the ABCD Vendor Views.

CELENT'S ABCD VENDOR VIEW

Celent has developed a framework for evaluating vendors. This is a standard representation of a vendor marketplace designed to show at a glance the relative positions of each vendor in four categories: Advanced and agile technology, Breadth of functionality, Customer base (i.e., relative number of customers), and Depth of client services. The Celent Vendor View shows relative positions of each solution evaluated and does not reflect an abstract evaluation. Each vendor solution is judged relative to the others in the group.

While this is a standard tool that Celent uses across vendor reports in many different areas, each report will define each category slightly differently. For this report, some of the factors used to evaluate each vendor are listed in Table 1. Celent's view of the relative importance of each factor and of the solution and vendor's capabilities also contributes to the final rating.

Table 1: Sample Celent ABCD Criteria

ABCD CATEGORIES	POSSIBLE FACTORS
ADVANCED TECHNOLOGY (AND FLEXIBLE TECHNOLOGY)	Platform and modernity (code base, platform, databases, localization capabilities, etc.)
	UI (Ease of use, configurability)
	Data and adaptability/extendibility (openness of application, code base, data model, etc.)
	Integration (Web services, APIs, reference comments)
	Scalability and cloud (cloud readiness, largest installations, etc.)
	Ease of change (upgrades, reference comments)
BREADTH OF FUNCTIONALITY	Functions and features provided in base offering
	In production lines of business and number of deployments for each
	User experience (reference comments)
CUSTOMER BASE	Number of live customers using the system
	Geographic footprint of the client base
	New client momentum
DEPTH OF CUSTOMER SERVICE	Size of professional services and support team
	Post-implementation experiences (reference comments)

Source: Celent

THE XCELENT AWARDS

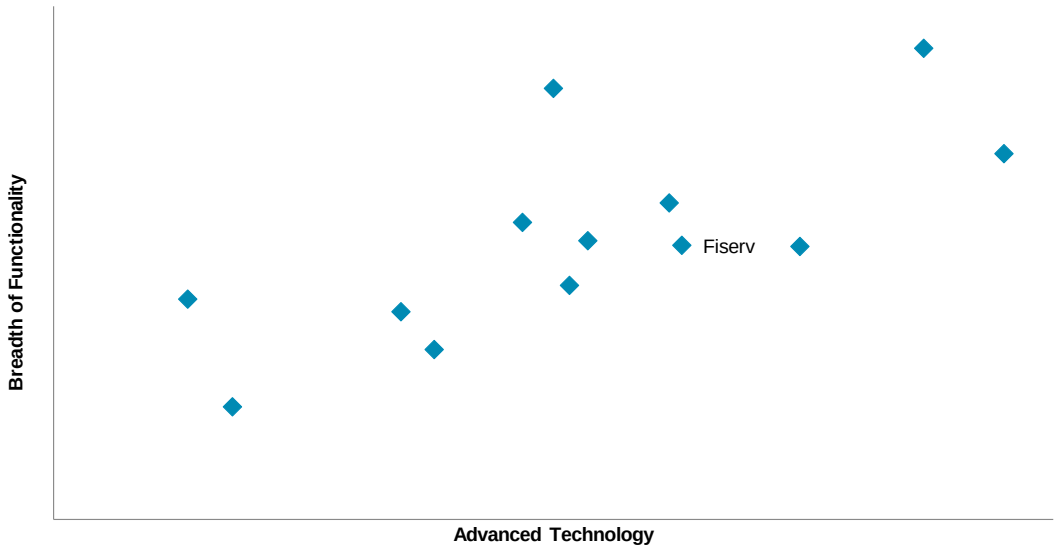
Within the above framework, the top performers in each of the ABCD dimensions receive a corresponding XCelent Award:

- XCelent Technology for the leading Advanced Technology score
- XCelent Functionality for the leading Breadth of Functionality score
- XCelent Customer Base for the leading Customer Base score
- XCelent Service for the leading Depth of Service score

XCELENT TECHNOLOGY AND XCELENT FUNCTIONALITY

Figure 2 positions each vendor along two dimensions: the vertical axis displaying the relative rankings for Advanced Technology and the horizontal axis showing relative Breadth of Functionality rankings.

Figure 2: XCelent Technology and XCelent Functionality

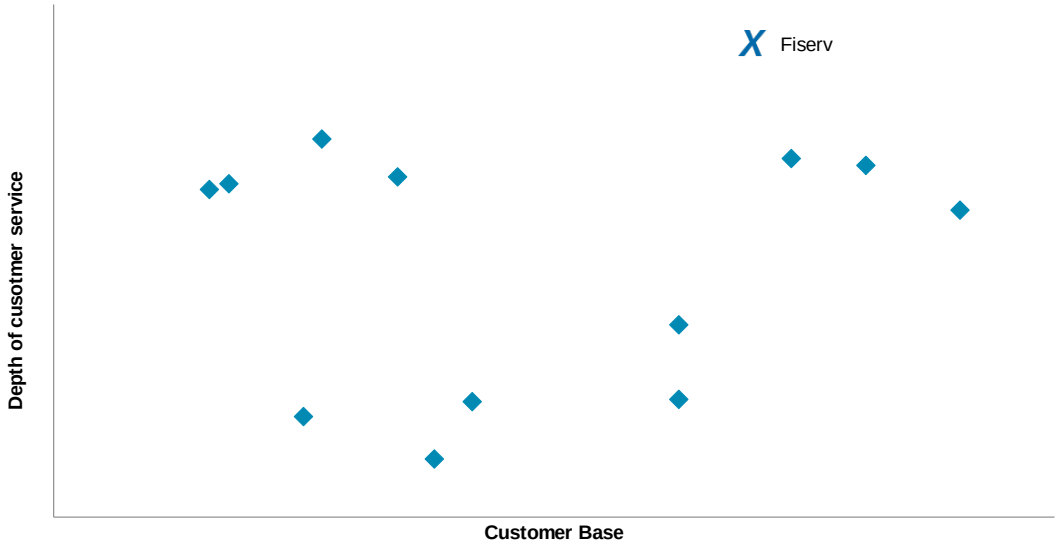


Source: Celent

XCELENT CUSTOMER BASE AND XCELENT SERVICE

Figure 3 positions each vendor along two dimensions: the vertical axis displaying the relative level of depth of customer service and the horizontal axis displaying the relative customer base. The XCelent Service winner is Fiserv.

Figure 3: XCelent Customer Base and XCelent Depth of Customer Service



Source: Celent

Celent advises financial institutions to consider past vendor results, but not to directly compare the placement of vendors in the charts from prior years, because not only is the market changing, but so has our analysis. The criteria used to determine the A, B, C, and D rankings in this report are broadly similar, but not identical, to the criteria used in the previous Celent AML vendor report published in 2012. For example, in this report, we are considering new criteria in Advanced Technology related to support for mobility, cloud, and unstructured data analysis. The market is also evolving due to acquisitions and partnerships, solutions development, and alternative delivery models.

We suggest that financial institutions consider their specific needs and each vendor for what it offers. Although they are very successful in one or more of the criteria, the XCelent Award winners may or may not be the best match for a financial institution's specific business goals and solution requirements.

VENDOR PROFILES

ABOUT THE PROFILES

Each of the profiles presents information about the vendor and solution; professional services and support capabilities; customer base; functionality and lines of business deployed; technology and partnerships; and implementations and cost.

As stated earlier, if a system was included in the ABCD Vendor View analysis, the profile also includes customer feedback; and Celent's opinion of the system with regards to usability, product configuration, and workflow capabilities, as well as summary comments.

Each profile includes a figure outlining available end-to-end components and the features and functions availability within the systems. The profiles also include tables and discussion regarding lines of business supported; scalability; currency and language support; technology and deployment options; the number of clients currently using the system; and other details.

For systems included in the ABCD Vendor View analysis, the vendor's reference feedback, gathered through an online survey, is presented in the profile. Customer feedback sections include a diagram that displays the average ratings given to the vendor in six categories. Each average rating includes up to 12 underlying ratings, as shown in Table 2, scored by the customer on a scale of 1 to 5, where 1 means poor and 5 is excellent. Open ended comments regarding the system and the vendor are also included in the feedback section.

It might be advisable to keep in mind that the evaluations and comments may vary according to the specific needs of each reference client.

Table 2: Customer Feedback Ratings

DIAGRAM AVERAGE (QUESTION ASKED)	RATINGS INCLUDED IN AVERAGE*
FUNCTIONALITY How would you rate the features and functions you are currently using?	Historical profiling of individual accounts Historical profiling of peer groups Rules and analytics What-if simulation and testing False positives reduction Case management Visualization tools Reporting Tools for managers Audit trail Support for channels and products Currency and language support

CONFIGURABILITY How would you rate the configurability of the system you are currently using?	Rules creation and maintenance Parameters and thresholds Workflow (design and maintenance) User interfaces (design and maintenance) Dashboards (design and maintenance) User management (permissions, authority) Reports (design and maintenance) Making minor changes Making major changes
INTEGRATION What has been your experience with the integration of this AML transaction monitoring system with other systems, tools, and data?	Your core processing systems Your onboarding and account opening systems Customer information files Other internal data sources External data sources Third party AML systems or analytics
TECHNOLOGY How would you rate the technology of this solution in the following areas?	Ease of system maintenance Flexibility of the data model Scalability of the solution Vendor's level of investment in improving technical performance through new releases and fixes Configurability of the solution Overall satisfaction with the technology
IMPLEMENTATION Thinking back to when you first implemented this AML transaction monitoring system, how would you rate this vendor in the following areas?	Responsiveness (handling of issue resolution) Project management (estimations, scope creep, etc.) Implementation completed on time Implementation completed on budget Overall project success Knowledge of your business Knowledge of their solution and relevant technology
SUPPORT How would you rate this vendor's support and overall professional services (after implementation) in the following areas?	Responsiveness (handling of issue resolution) Speed of issue resolution Project management (estimations, scope creep, etc.) Work completed on time Work completed on budget Knowledge of your business Knowledge of their solution and relevant technology Consistently meeting SLAs Overall quality of professional services

Source: Celent
*Scale 1 to 5, where 1 is poor and 5 is excellent. "No Opinion" not included in average.

When discussing customers of the various solutions, we have used the tier definitions in Table 3.

Table 3: Financial Institution Tier Definitions Used in This Report

TIER	DEFINIITION
1	Clients with US$100 billion or more in assets (for insurers: US$5 billion or more in premiums)
2	Clients with US$50 billion to US$99.9 billion in assets (for insurers: US$1 billion to US$4.9 billion in premiums)
3	Clients with US$10 billion to US$49.9 billion in assets (for insurers: US$500 million to US$999 million in premiums)
4	Clients with US$1 billion to US$9.9 billion in assets (for insurers: US$100 million to US$499 million in premiums)
5	Clients with under US$1 billion in assets (for insurers: under US$100 million in premiums)

Source: Celent

Concerning implementation costs and fees, Celent asked vendors to provide implementation costs (work by the financial institution, vendor, or third parties) for two hypothetical financial institutions:

- Regional Bank A, with four lines of business and total assets of US$25 billion.
- Bank Holding Company B, with four companies, operations in five or more countries, and combined total assets of US$125 billion.

FISERV: AML RISK MANAGER

XCELENT Service 2018

COMPANY AND PRODUCT BACKGROUND

Fiserv is a publicly traded company headquartered in Brookfield, WI, USA with regional headquarters in London, England, Mexico City, and Singapore. Fiserv has an additional 40 offices in the US and a presence in 110 cities globally. Total corporate revenues of Fiserv are US$5.7 billion; the firm does not disclose the revenues attributable to its financial crime solutions. The company has some 25,000 employees, of which 500 in the Fiserv Risk & Compliance business unit are responsible for the development, implementation, and support of the Financial Crime Risk Management (FCRM) suite of solutions.

AML Risk Manager is a module of Fiserv's end-to-end FCRM suite. It was first deployed for a financial institution in 1999 and released in 2001. The last major release was FCRM Version 5.6. in March 2018. The technology changes in that release included configurable KYC questionnaires, extended Beneficial Ownership analysis and visualization, enhanced real-time detection featuring a complex event processing engine supporting flexible event modelling; user-configurable scenarios; and a data mart and reporting tools to support customer management and regulatory reporting.

Recent acquisitions by Fiserv relevant to the AML/KYC space include Monitise and Dovetail. For example, Dovetail can feed payments transactions into FCRM solutions for monitoring and screening.

Competitors cited by Fiserv in the AML transaction monitoring space include BAE Systems, NICE Actimize, Oracle, and SAS Institute.

Table 4: Company and Product Snapshot

COMPANY	Corporate name	Fiserv
	Annual corporate revenues	US$5.7 billion
	Year founded	1984
	Exchanges/Symbols	NASDAQ: FISV
	Headquarters	Brookfield, WI, USA
AML TRANSACTION MONITORING PLATFORM	Name	AML Risk Manager
	Current release (date of release)	FCRM Version 5.6 (March 2018)
	Last major release	FCRM Version 5.6 (2018)
	Target market	Regional and global financial services companies; consultancies (for lookbacks and AML program reviews)

Source: Fiserv RFI

OVERALL FUNCTIONALITY

Figure 4: Functionality

SUITE FUNCTIONALITY	FEATURES AND FUNCTIONS		
Transaction Monitoring	Real-time transaction monitoring	Monitors all transactions	Rules engine
	Historical profiling, account level	Historical profiling, peer group	Rules creation
	Link analysis	Searchable rules repository	Rules simulation
Watchlist Screening	See Celent report, Solutions for Watchlist Screening: 2018 ABCD Vendor View		
Onboarding / Customer Due Diligence			
Case Management	Alert risk scoring	Attachments, documents	Attachments, image, audio, and video files
	Case assignment & queueing	Manual email notifications	Automatic email notifications
	Escalations	Visualization tools	Compliance dashboard
	Supports output from 3rd party TM systems	Integrated fraud/AML case management	
Reporting	Regulatory reporting	Auto-generation of regulatory reports	E-regulatory filing
	Prepackaged management reports	Custom report generation	
	Audit trail, user activity	Audit trail, system modifications	

Source: Fiserv RFI

CELENT OPINION

Fiserv AML Risk Manager was originally developed under the name ERASE by NetEconomy, a software vendor specializing in financial crime technology that was acquired by Fiserv in 2007. While continuing to sell AML Risk Manager globally, Fiserv also offers the solution on an ASP basis to its core processing clients in North America, which accounts for the bulk of its sizable customer base.

The vendor states that 25% of its on-premise clients use the solution in multiple countries, including 30 clients using it in five to 10 sites and five clients using it across 10 to 34 sites. Implementation models for these deployments include multiple countries hosted at one data center hub, multiple countries hosted on a commercial private cloud platform, and single-country implementations.

AML Risk Manager is unique in containing two transaction monitoring engines: the legacy monitoring engine, used for batch monitoring, and a recently developed complex event processing (CEP) engine that supports advanced analytics including Predictive Model Markup Language (PMML) models and real-time monitoring.

The solution provides a variety of visual tools, including link analysis of transactional as well as non-financial relationships such as address; geographic heat maps; and a visualization tool capable of depicting beneficial ownership shares in an entity, as well as performing link analysis on the beneficial owners.

Items on the roadmap for AML Risk Manager include mobile device support; Japanese language support; enhancements to case management; and expanded risk assessment reporting. Analytics enhancements on the roadmap include predictive analytics for customer and alert scoring; automated closing of alerts using robotics; and machine learning / AI capabilities.

RULES AND ANALYTICS

The AML Risk Manager transaction monitoring product has a library of some 300 pre-programmed scenarios for AML covering products, channels, and business types. Rules are often tied to regulations in specific jurisdictions or guidance from global compliance organizations. The product also supports scenario creation by business users.

The solution's analytics include behavioral analytics based on customer, account, and peer profiling and statistical analytics based on custom models, e.g., predictive analytics models.

The solution takes a layered approach to monitoring by analyzing transactions against historical behavior, expected behavior, and peer group behavior.

FALSE POSITIVES MANAGEMENT

According to the vendor, false positive rates achieved by AML Risk Manager cover a wide range, from 1% to 25%, depending on specific configurations based on risk assessment. Technology features designed to reduce false positives include risk scorecards, peer group analysis, and simple rules. A key technique of the solution is entity profiling to construct typical behavior patterns against which new activity is compared. These profiles can include amount and frequency of transactions, types of transactions, source and destination of transaction, and non-financial activity.

At the post-processing level, an Automated Alert Investigation (AAI) feature utilizes robotic processing automation (RPA) and machine learning to prioritize alerts based on previous alert decisions, to drive workflows, and to automatically close alerts. The solution also provides reports analyzing false positive rates for alerts and cases to support the fine tuning of scenarios by permissioned users.

Regulatory Reporting

Fiserv's support for regulatory reporting is outlined in the table below.

Table 5: Regulatory Reporting Support Details

CATEGORY	SUPPORTED TYPES
REGULATORY REPORTING	- SARs, CTRs for 20+ countries - EFT, goAML, CRS, FATCA
REPORT AUTO-GENERATION, PDF	OFAC Transaction Reports
REPORT AUTO-GENERATION, OTHER FORMATS	Supported and already in production
GOVERNMENT E-FILING PROGRAMS SUPPORTED	US FinCEN; Canada FINTRAC; goAML (multiple countries)

Source: Fiserv RFI

Lines of Business and Products Supported

AML Risk Manager currently supports banking, insurance, prepaid cards, money services, asset management, casinos, payments, brokerage, and corporates at live clients. Support for channels, products, transactions, and message types is listed in the table below.

Table 6: Product Support Details

CATEGORY	SUPPORTED TYPES
DELIVERY CHANNELS	Branch, ATM, internet, mobile, agents
FINANCIAL PRODUCTS	A range of financial products
TRANSACTIONS	A range of internal, external, financial, and non-financial transaction types. New transaction types can be defined by users
MESSAGE TYPES	SWIFT, Fedwire, ACH, SEPA, Faster Payments

Source: Fiserv RFI

AML Risk Manager supports multiple currency and built-in currency conversion. All standard currencies are supported at live clients. Recent implementations include transactions in cryptocurrencies and exchange between fiat and cryptocurrencies.

The system supports multiple languages. Languages that are supported at live clients include English, Dutch, French, Portuguese, Polish, Russian, Spanish, and simplified Chinese.

Customer Base

Fiserv has a total of 1,200 clients worldwide in production with their AML transaction monitoring system in more than 70 countries. The breakdown by financial sector, tier, and geography is given in the table below. The customer figures are skewed to the US and Canada due to Fiserv's presence in core processing in these countries; however, Fiserv has implementations globally.

Table 7: Client Breakdown

SECTOR		TIER		REGION	
Retail/corporate banks	91%	Tier 1	3%	US/Canada	84%
Investment banks	3%	Tier 2	5%	Latin America	1%
Asset managers	1%	Tier 3	9%	Asia	4%
Insurers	3%	Tier 4	8%	Europe	8%
Other firms	2%	Tier 5	75%	Middle East	2%
				Africa	1%
				Rest of World	0%

Source: Fiserv RFI

Ninety-five percent of Fiserv's transaction monitoring clients also use the vendor's watchlist screening module; 98% of Fiserv's transaction monitoring clients also use the vendor's case management module; and 98% of Fiserv's clients are using the vendor's compliance dashboard.

The release versions of AML Risk Manager used by customers are broken out in the table below.

Table 8: Customer Base

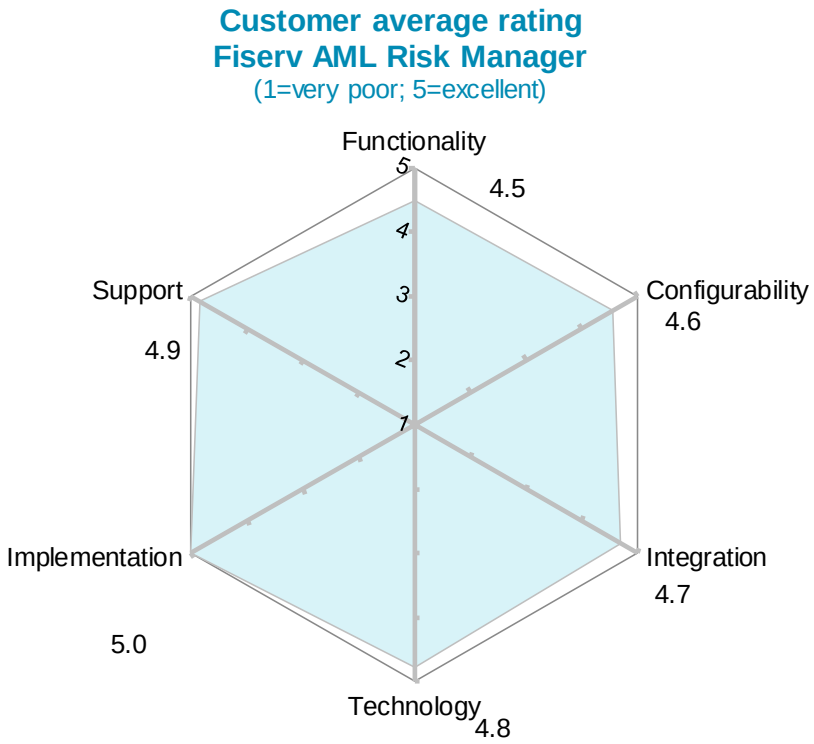
DEPLOYMENT CATEGORY	NUMBER OF CLIENTS
IN PRODUCTION WITH RELEASE OF LAST MAJOR CHANGE	800
IMPLEMENTING RELEASE OF LAST MAJOR CHANGE	200
IN PRODUCTION WITH PRIOR RELEASE	200
NEW CLIENTS SINCE 2014	270
DEPLOYMENT METHOD (PERCENTAGE OF CLIENT BASE)	On Premise: 40% Off-premise (hosted, SaaS, cloud): 60%

Source: Fiserv RFI

CUSTOMER FEEDBACK

Three clients provided feedback on Fiserv. Two are tier 1 institutions. One is a tier 3 institution. One client uses the system in the US and/or Canada for insurance. Another uses the system in the US and/or Canada for retail banking, corporate banking, and investment banking / brokerage. The last uses the system in Europe for retail banking, corporate banking, and insurance. All three have used Fiserv for more than three years.

Figure 5: Customer Feedback



Source: 2018 Celent AML Transaction Monitoring customer feedback survey. N = 3

Clients rated Fiserv strongly overall. In the area of functionality, clients liked the historical profiling of individual accounts; while currency and language support was seen as an area of relative improvement. In terms of usability (configurability), rules creation and maintenance, parameters and thresholds, user management (permissions, authority), and making minor changes were highlighted; while reports (design and maintenance) and making major changes were areas of relative weakness. Within technology, ease of system maintenance, scalability of the solution, and overall satisfaction with the technology were scored the highest; and vendor's level of investment in improving technical performance through new releases and fixes was seen as weaker.

Clients felt the solution integrated most easily with their customer information files and integrated less well with their core processing systems, external data sources, and third party AML systems or analytics.

Regarding their implementation experience, the three reference clients gave Fiserv highest marks across the board (a perfect 5).

Finally, in the area of ongoing system support, responsiveness (handling of issue resolution), project management (estimations, scope creep, etc.), work completed on budget, vendor's knowledge of the client's business, and overall quality of support received the highest scores; while speed of issue resolution, work completed on time, vendor's knowledge of the solution and relevant technology, and consistently meeting SLAs were given somewhat lower marks.

Clients said the two or three best things about Fiserv AML Risk Manager were its real-time capability; comprehensiveness, scalability, flexibility, and ability to identify unusual activity across multiple silos, channels, and product lines; continual risk profiling, monitoring, and scoring based on static and dynamic information; ease of case

management in holistically monitoring and investigating AML and fraud on one platform; and the responsiveness and competence of support and services. Suggested areas for improvement were scenario development and standardization; custom regulatory reporting; and sharing of user group data to aid in peer-based tuning and predictive modeling.

TECHNOLOGY

Technology details for AML Risk Manager are provided in the table below.

Table 9: Technology Options

TECHNOLOGY	SPECIFICS
USER INTERFACE	Business Users: 100% Browser-Based (HTML 5) Developers: 100% Browser-Based (HTML 5)
CODE BASE	Core technology: .NET: 100% Business users: .NET: 50% SQL: 50% Developers: .NET: 50% Visual Basic: 10% JavaScript: 10% SQL: 30%
OPERATING SYSTEMS	Preferred: Windows (only option) Additional: None
APPLICATION SERVERS	Preferred: Windows Server/.NET (only option) Additional options: None
DATABASES	Preferred: Microsoft SQL Server (only option) Additional options: None
INTEGRATION METHODS	Preferred: SOA/Web Services; Flat files; Additional options: XML; other markup language; RESTful HTTP style services; MQSeries, JMS or similar queue technology; custom API; ESB architectures
DATA MODEL	Fiserv releases the data model to clients.

Source: Fiserv RFI

The scalability achieved by Fiserv's transaction monitoring engine is shown below.

Table 10: Scalability

LIVE CLIENT	Daily transactions at largest live client implementation: 30,000,000 Concurrent users at largest live client implementation: 200
LAB ENVIRONMENT	Highest daily transactions in lab environment: 30,000,000 Most concurrent users in lab environment: 300

Source: Fiserv RFI

Data sources that can be analyzed by the transaction monitoring engine include: structured data; and unstructured data - text. The system can support analysis of audio by converting it to text. Video analysis by third party solutions can be integrated into case management workflows.

The solution's support for user access and permissions functionality is shown in the table below.

Table 11: Access and Permissions

FUNCTION	AVAILABILITY
SUPPORTS SINGLE-SIGN ON (SSO)	Supported and already in production
MANAGEMENT OF PERMISSIONS AND ROLES POSSIBLE AT INDIVIDUAL AND GROUP LEVEL	Supported and already in production
FUNCTIONS TO BE USED CAN BE CONTROLLED AT USER LEVEL	Supported and already in production
ACCESS CONTROL POSSIBLE AT DATA ITEM LEVEL AND RECORD LEVEL	Supported and already in production
AUDIT TRAIL LOG	Supported and already in production

Source: Fiserv RFI

Deployment options supported by Fiserv's transaction monitoring solution are shown in the table below. There is no preferred method of deployment.

Table 12: Deployment Options

DEPLOYMENT MODE	AVAILABILITY
ON PREMISE	Yes
HOSTED	Yes
CLOUD	Yes
HYBRID CLOUD	Yes

Source: Fiserv RFI

PARTNERSHIPS

Fiserv has established system integration partnerships. Partners include ACA Televance, Alvarez and Marsal, Belleron, HS Data, ION, Iovation, and K2. The vendor is open to working with clients' preferred integrators.

IMPLEMENTATION, PRICING, AND SUPPORT

The vendor has 191 employees available to provide professional services / client support for the product. These professional services / client support staff average seven years of experience.

A typical project team of six people consists of 40% vendor resources, 50% client resources, and 10% resources from a systems integrator.

The average time to get the system up and running in a single jurisdiction is typically four to six months, depending on the integration requirements and the level of configuration required.

Fiserv offers a perpetual license; a term license; SaaS (system hosting and maintenance and usage-based license); and transaction based-licensing as pricing options; as well as additional license models based on client needs. The license fees can be based on factors including transaction type and volume; number of concurrent users; number of total or named users; data volume; firm asset size; and enterprise license / flat fee. Risk/reward pricing, with some proportion of license fees deferred until benefits realization, is available from this vendor.

The total cost to implement AML Risk Manager can vary according to the capabilities and available resources of the client, and the overall scope of system use. Fiserv has not provided pricing estimates, but believes its pricing is competitive in all markets and driven by a philosophy of value pricing.

Table 13: Implementation Cost Estimates

SCENARIO	LICENSING	VENDOR FEES	INTERNAL COSTS	MAINTENANCE FEE / OTHER
FOR REGIONAL BANK A, with four LoBs and total assets of US$25 billion	N/A	N/A	N/A	--%
FOR BANK HOLDING COMPANY B, with four companies, operations in five countries, and combined total assets of US$125 billion	N/A	N/A	N/A	--%

Source: Fiserv RFI

CONCLUDING THOUGHTS

AML compliance is a complex area, and there are no magic bullets. The field is also entering a new era of competition. Herewith are some suggestions for navigating the space.

FOR FINANCIAL INSTITUTIONS

There is no single best anti-money laundering solution for all financial institutions. There are a number of good choices for a financial institution with almost any set of requirements. An organization seeking a new AML system should begin the process by looking inward. Every firm has its own unique mix of lines of business, geography, staff capabilities, business objectives, and financial resources. This unique combination, along with the organization's risk appetite, will influence the list of vendors for consideration.

Some vendors are a better fit for a company with a large IT group that is deeply proficient with the most modern platforms and tools. Other vendors are a better fit for a firm that has a small IT group and wants a vendor to take a leading role in maintaining and supporting its applications.

Most AML systems bring some level of out-of-the-box functionality for various lines of business and operating models. Systems may also offer configuration tools to build capabilities for both known and future requirements.

We recommend that financial institutions that are looking for an AML system narrow their choices by focusing on four areas:

- The functionality needed and available out of the box for the lines of business and states desired. Check to see what is actually in production.
- The technology — both the overall architecture and the configuration tools and environment.
- The vendor's stability, knowledge, and investment in the solution.
- Implementation and support capabilities and experience.

FOR VENDORS

As a group, vendors continue to make significant investments in their AML systems. The solutions are delivering more functionality, improving configuration tools, and starting to leverage advanced technologies. Although these trends are all very good news for financial institutions, they do make the competitive challenges facing vendors that much more daunting.

Celent recommends vendors differentiate themselves by:

- Focusing on improving usability for both new and experienced users and managers.
- Making implementation faster and less expensive.
- Continuing to build out advanced capabilities; as well as configurablity to put change controls in the hands of the client.

Was this report useful to you? Please send any comments, questions, or suggestions for upcoming research topics to info@celent.com.

LEVERAGING CELENT'S EXPERTISE

If you found this report valuable, you might consider engaging with Celent for custom analysis and research. Our collective experience and the knowledge we gained while working on this report can help you streamline the creation, refinement, or execution of your strategies.

SUPPORT FOR FINANCIAL INSTITUTIONS

Typical projects we support related to anti-money laundering compliance include:

Vendor short listing and selection. We perform discovery specific to you and your business to better understand your unique needs. We then create and administer a custom RFI to selected vendors to assist you in making rapid and accurate vendor choices.

Business practice evaluations. We spend time evaluating your business processes, particularly regulatory and compliance areas supported by technology. Based on our knowledge of the market, we identify potential process or technology constraints and provide clear insights that will help you implement industry best practices.

IT and business strategy creation. We collect perspectives from your executive team, your front line business and IT staff, and your customers. We then analyze your current position, institutional capabilities, and technology against your goals. If necessary, we help you reformulate your technology and business plans to address short-term and long-term needs.

SUPPORT FOR VENDORS

We provide services that help you refine your product and service offerings. Examples include:

Product and service strategy evaluation. We help you assess your market position in terms of functionality, technology, and services. Our strategy workshops will help you target the right customers and map your offerings to their needs.

Market messaging and collateral review. Based on our extensive experience with your potential clients, we assess your marketing and sales materials — including your website and any collateral.

RELATED CELENT RESEARCH

Dawn of a New Era in AML Technology
September 2018

Robotic Process Automation in Risk and Compliance
August 2018

AI Made to Reduce False Positives Part 2: Vendor Spectrum
July 2018

AI Made to Reduce False Positives, Part 1: Detection Capabilities and Use Cases
May 2018

Digital Identity as a Tradable Asset
May 2018

Claims Fraud Detection Systems: 2018 IT Vendor Spectrum
May 2018

Risk Management and Compliance 2018: CROs Navigate NextGen Tech
May 2018

Achieving Holistic AML: Focus on Watchlist Screening
March 2018

Capital Markets Surveillance Vendor Landscape: The Next Wave in Trade and Communication Surveillance
February 2018

Innovations in AML and KYC Platforms: New Models Powered by Advanced Computing
January 2018

Innovation in AML Technology: New Tools for Optimizing Compliance Efficiency
November 2017

A New Era in Capital Markets Surveillance: As Far as the AI Can See
November 2017

Cloud-Enabled Governance, Risk, and Compliance Solutions
October 2017

Copyright Notice

Prepared by

Celent, a division of Oliver Wyman, Inc.

For more information please contact info@celent.com or:

Neil Katkov nkatkov@celent.com

AMERICAS

USA

200 Clarendon Street, 12th Floor
Boston, MA 02116

Tel.: +1.617.262.3120
Fax: +1.617.262.3121

USA

1166 Avenue of the Americas
New York, NY 10036

Tel.: +1.212.541.8100
Fax: +1.212.541.8957

USA

Four Embarcadero Center, Suite 1100
San Francisco, CA 94111

Tel.: +1.415.743.7900
Fax: +1.415.743.7950

Brazil

Av. Doutor Chucri Zaidan, 920 –
4º andar
Market Place Tower I
São Paulo SP 04578-903

Tel.: +55.11.5501.1100
Fax: +55.11.5501.1110

EUROPE

France

1 Rue Euler
Paris
75008

Tel.: +33.1.45.02.30.00
Fax: +33.1.45.02.30.01

United Kingdom

55 Baker Street
London W1U 8EW

Tel.: +44.20.7333.8333
Fax: +44.20.7333.8334

Italy

Galleria San Babila 4B
Milan 20122

Tel.: +39.02.305.771
Fax: +39.02.303.040.44

Switzerland

Tessinerplatz 5
Zurich 8027

Tel.: +41.44.5533.333

ASIA

Japan

The Imperial Hotel Tower, 13th Floor
1-1-1 Uchisaiwai-cho
Chiyoda-ku, Tokyo 100-0011

Tel: +81.3.3500.3023
Fax: +81.3.3500.3059