CELENT

XCELENT Awards 2018

SOLUTIONS FOR WATCHLIST SCREENING

2018 ABCD VENDOR VIEW

Neil Katkov, PhD
November 2018

This is an authorized excerpt from a Celent report profiling watchlist screening vendors. The reprint was prepared for Fiserv, but the analysis has not been changed. For more information about the full report, please contact Celent at info@celent.com.

CONTENTS

INTRODUCTION

In recent years, watchlist screening has become the most scrutinized area of anti-money laundering (AML) compliance, and the area that has been hit with the most outsized fines by regulators. In a sense, this is simply because identifying known bad actors and understanding the potential risk of customers and counterparties forms the core of any anti-money laundering effort.

From the operational point of view, customer screening is a crucial operation because it forms a central part of every stage in the AML compliance chain, from onboarding all the way through to case investigation.

The core mission of anti-money laundering programs is to identify risky actors and detect suspicious activity. This is accomplished through three key operational areas: entity review, payments screening, and forensics. In an effective AML program, these three areas will be interlocking, with risk findings from each area informing the others. Watchlist screening provides inputs to all three of these areas.

Financial institutions must screen customers and/or counterparties at every stage of the AML compliance value chain. This includes during know your customer (KYC), customer due diligence (CDD) and enhanced due diligence (EDD) checks and periodic customer reviews; as well as when initiating wires and other payments. Watchlist screening is also an important component of ongoing transaction monitoring.

Figure 1: Watchlist Screening in the AML Value Chain

Entity Review	Payments Screening	Forensics
Onboarding/KYC, PEPs	Sanctions/Embargo (international wires)	Transaction Monitoring / Detection
Risk Profiling / Customer Due Diligence	ACH, Domestic Wires	Investigation / Enhanced Due Diligence
Customer Review	High-Value Payments	Prevention

Source: Celent

Some of the challenges in watchlist screening and entity review that are begging for effective solutions include:

- Positive identification of sanctioned entities and politically exposed persons (PEPs).
- Resolution of name variations, including aliases, transliterated names, and names in non-Latin scripts; as well as variations due to data quality issues such as partial names and corrupted names.

- Risk profiling, assessment, and scoring during the onboarding process as well as periodic customer reviews.
- Reduction of false positive rates, which can reach 70% of alerts or even higher.
- Growing speed of payments and transactions in the context of digitization, Fintech, and e-commerce; and expectation of faster onboarding for online products and services.
- Multitude of and rapidly changing watchlists.
- UBO requirements, data for which are not easily available.

Emerging technology such as artificial intelligence (AI) and robotic process automation (RPA) hold 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 next-gen tech.

Such is the environment surrounding this, Celent's fourth review of watchlist screening software systems available to financial institutions (a companion report evaluates providers of AML 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 watchlist screening 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.

Watchlist screening 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 rollups; and other features to support increased efficiency at the alert investigation and case management level.

Importantly, watchlist screening software providers are now developing new capabilities leveraging next-generation technologies. These new capabilities, catalogued in this report, include: post-screening analytics; automated alert closing using machine learning and robotic process automation (RPA); unstructured data analysis; and natural language generation.

AML SOLUTIONS: DEFINITION AND FUNCTIONALITY

Key Research Question 1

What is a watchlist screening system?

Watchlist screening systems match customers, counterparties, and other entities against lists issued by governments or regulatory bodies (official watchlists), entity datasets offered by commercial providers, internal lists, or open source intelligence. Watchlist screening use cases include customer due diligence for onboarding or periodic customer review, payments screening, and other routines to support regulatory compliance.

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 watchlist screening for payments and wires, onboarding, customer due diligence (CDD), and other know your customer (KYC) processes, as well as transaction monitoring. 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 watchlist screening (WL), 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 Anti-Money Laundering: 2018 Transaction Monitoring ABCD Vendor View*, evaluates transaction monitoring (TM) capabilities, as well as related case management and reporting functionality.

Figure 2 displays some of the specific features in each suite-level category used to evaluate watchlist screening 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 2: Watchlist Screening System Key Modules and Features

SUITE CATEGORIES	FEATURES AND FUNCTIONALITY		
Transaction Monitoring	See Celent report, Solutions for Anti-Money Laundering: 2018 Transaction Monitoring ABCD Vendor View		
Watchlist Screening	Real-time sanctions dispositioning	Real-time domestic payments dispositioning	Screening support for double-byte scripts
	Screening of external data sources	Automated download of watchlists	Automated delta updates
	Data cleansing / deduping	White list management	Support for internal lists
Onboarding / Customer Due Diligence	Risk scoring for onboarding	Risk scoring for customer review	Account opening checklist workflow
	STP integration with account opening systems	STP integration with core systems	STP integration with TM systems
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
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

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. The WL engine generates alerts when it has identified a potential match of an entity against a watchlist. Many systems will also assign a score to the alert indicating the strength of the match. These alerts are then fed into a case management system (or, in the case of payments screening, into a real time decisioning module) for review by compliance analysts.

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.

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.

Transaction monitoring. Transaction monitoring refers to the periodic analysis of financial and non-financial 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.

Many transaction monitoring software vendors offer versions of their solution for multiple use cases — such as anti-fraud, counter terrorist financing, or trade surveillance — in addition to AML. The transaction monitoring functionality of AML vendors is profiled in the companion Celent report, *Solutions for Anti-Money Laundering: 2018 Transaction Monitoring ABCD Vendor View.*

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 WL systems' output to increase system efficiency through post-processing (that is, post-WL) 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 OFAC reports, 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: KEY FEATURES

Below we highlight some of the specific features and functionality that support best practice watchlist screening 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.

Screening Engine Features

The types of algorithms, workflow, and connectivity available, and the tools provided to manage these, can differentiate watchlist screening systems.

Support for watchlists. Solutions vary in the type and number of watchlists they support. Firms operating in one market may only require support for a limited number of official watchlists, while multinational firms may benefit from a broader range of supported lists. Support for large commercial data sets, such as PEPs or adverse media lists, may also be a requirement. Support for lists is not necessarily plug and play. Optimized connectors and translators for watchlists can result in faster throughput and enhanced analytic efficacy. Out-of-the-box support for specific lists can reduce implementation time and maintenance costs.

Watchlist management. Features designed to help firms maintain watchlist data include automated or assisted download of watchlists from official and commercial providers as well as data cleansing routines such as removing duplicated data (deduping) and delta updates. Additionally, some vendors provide curated watchlist sets that are updated, cleansed, and configured for consumption by the vendor's screening solution.

Real-time payments screening. Sanctions screening is a crucial watchlist use case for firms involved in international payments. Sanctions violations have resulted in the most severe regulatory penalties in AML, with fines reaching billions of dollars. Domestic payments screening is also increasingly important from the compliance perspective and for tackling fraud.

Real-time payments screening requires a) connectivity to payments gateways and b) workflow to govern the pass, block, or review process. Some WL systems can be directly integrated with payments gateways or are SWIFT-certified; while others connect to payments software that in turn connect to the gateways. Workflow support may include enhanced features such as intraday escalation and time management to facilitate processing of alerts to meet payments cut-off deadlines.

Matching Algorithms. Collectively, vendors offer a panoply of algorithms, routines, and analytics designed to detect and score name matches. This includes standard algorithms such as the various Soundex and distance algorithms; fuzzy logic; proprietary algorithms; language- or culture-specific matching routines; algorithms sourced from third party vendors; token libraries; and other techniques.

Some vendors have spent considerable time and effort in building up extensive libraries of algorithms and tokens and devising unique analytic approaches to scoring matches. Vendors may offer the capability to match multiple data fields including addresses, DoB, and other information in addition to names, or to match against unstructured data in addition to structured data.

Business rules. Rules in the watchlist context are often used to orchestrate screening routines according to the user's risk policies and operational procedures. These rules may be applied prior to screening of after screening takes place. Examples of pre-screening rules include rules that route transactions to payment systems according to currency, jurisdiction of the counterparty, or other parameters; or that trigger alerts for transactions that meet specified criteria, such as wires to sanctioned countries. Post-screening rules may route alerts to analyst teams according to factors such as match score (priority) and alert volumes.

Rules may also be available to configure screening runs by, for example, invoking specific watchlists to screen against, such as local jurisdiction lists; or deploying specific algorithms from the solution's available library.

Language support. Support for multiple languages can be a requirement for multinational banks as well as for home market banks engaged in international payments or supporting an international clientele. Language support varies among solutions and can include localized user screens, display capability for multiple languages, or full data screening capability for multiple languages. Depending on the solution, multi-lingual screening capability may rely on screening transliterations of the original language data or may involve direct screening of the original language input. Additionally, as mentioned above, some solutions apply language-specific routines to the matching process.

Firms may have requirements for processing specific non-Latin scripts such as Arabic or Cyrillic, as well as for double-byte character sets such as Chinese or Japanese. Here too, capabilities range from simple display of the scripts to full screening capability.

False positives reduction. The large number of false positive alerts typically generated by watchlist screening systems creates substantial operational and cost burdens for financial institutions. False positives reduction features are therefore important capabilities in a watchlist screening system. Watchlist screening systems may apply various techniques prior to, during, and after the screening process. False positives reduction techniques include parameter tuning, configurable algorithm selection, white lists, alert suppression, alert prioritization, alert triage, and post-screening analytics.

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

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. Support capabilities may vary depending on the use case. For example, sanctions screening workflow is typically limited to supporting the pass-or-block process, whereas screening for onboarding or customer review may require more robust investigative workflow.

Workflow. Effective workflow for alert and case investigation is crucial for supporting accurate and efficient watchlist screening operations. Depending on the needs of the financial institution, both predefined workflows to support specific use cases (for example, sanctions screening as well as screening for customer review), as well as configurable workflow and user-definable screens may both 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 are 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 visualization of links and networks, plug-ins such as embedded Google maps, and links to external data sources.

Attachments. Most systems provide open text windows for analysts to insert ad hoc notes; and may have 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.

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 systems, such as AML and fraud systems in addition to watchlist screening systems; as well as line-of-business or regional systems.

False positives reduction. Post-processing (post-screening) 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

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 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, are important to support best practices in internal employee and IT governance, external audit, and regulatory compliance.

Technology Features

Real-time processing. The ability to screen against watchlists and dispose resulting alerts on an intraday basis has long been a requirement for payments screening, particularly sanctions screening. Now, an increased regulatory focus on domestic payments; the advent of alternative payments, online lifestyle services, and fintech; as well as the movement in a number of markets toward faster payments are increasing the need for real-time screening capabilities. In addition to real-time connectivity, supporting

these newer use cases may require big data analytics, AI, and robotics to support faster decisioning.

Data types. Watchlist screening has traditionally involved analysis of financial and non-financial transaction data resident in core systems, customer information files, the watchlist data itself, and other structured data sources. At the same time, unstructured data is an increasingly important requirement for many firms. Watchlist screening has long relied on a wide variety of publicly available data, such as bankruptcy lists, as well as commercial datasets. The value of alternative data, such as adverse media, in assessing risk; the relevance of information found in PDF files such as incorporation documents; the growing need for new data sources covering areas such as beneficial owners, small businesses, and international jurisdictions; and new analytic techniques such as graph analysis are all driving increased interest in unstructured data analysis.

System access and permissions. Support for access roles and permissions is important for watchlist screening 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 watchlist screening solution 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 watchlist screening technology space is poised for rapid evolution, with advanced technologies including artificial intelligence, machine learning, robotic process automation, and natural language understanding/generation all being deployed in efforts to optimize screening operations. The profiles in this report point out the steps watchlist screening solution vendors are taking to incorporate these emerging technologies into their offerings.

REPORT METHOD

Key Research Question 2

Who are the leading watchlist screening system vendors globally?

This report profiles 20 watchlist screening systems and indicates the global footprint of their solutions by region; 16 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 20 watchlist screening 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, a watchlist screening 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 two reference customers.

There are 16 solutions that meet these criteria and are included in this report with ABCD profiles.

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 four solutions in this category.

EVALUATION PROCESS

Celent sent a detailed request for information to a broad set of watchlist screening 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 and distribution 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, etc.)
	UI (Ease of use, configurability)
	Data and adaptability/extensibility (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, features, and analytics 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 and business sectors 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

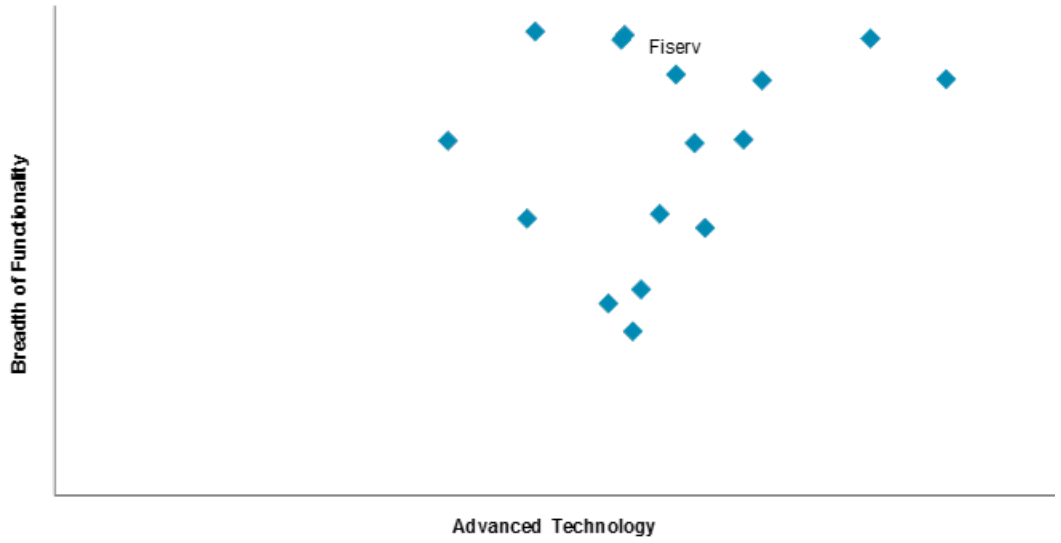
Within the above framework, the top performers in each of the ABCD dimensions receive a corresponding XCelent Award:

- 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 3 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 3: Watchlist Screening ABCD — Advanced Technology and Breadth of Functionality

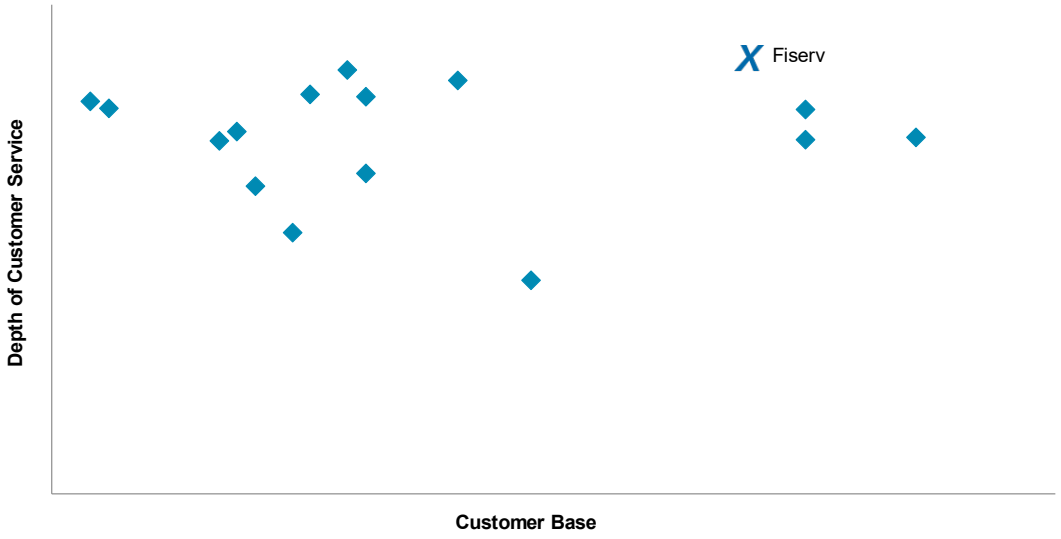


Source: Celent

XCELENT CUSTOMER BASE AND XCELENT SERVICE

Figure 4 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 award goes to Fiserv.

Figure 4: 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 five categories. Each average rating includes up to 17 underlying ratings, as shown in Table 3, 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?	Domestic payments screening
	Sanctions screening
	Real-time sanctions and payments dispositioning
	Screening for KYC/CDD
	Screening for customer review
	Name-matching algorithms and analytics
	False positives reduction
	Support for official watchlists
	Support for commercial databases such as PEPs
	Screening of adverse news, social data, and other unstructured data sources
	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 watchlist screening system with other systems, tools, and data?	Your payments systems
	Your onboarding and account opening systems
	Customer information files
	Other internal data sources
	External data sources
	3rd 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, Wisconsin, US 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 matching algorithms to reduce false positives, and enhanced real-time interdiction capabilities for SWIFT messaging with specific SWIFT message display screens.

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 watchlist screening space include Accuity, LexisNexis, and Thomson Reuters.

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
WATCHLIST SCREENING PLATFORM	Name	AML Risk Manager
	Current release (release date)	FCRM Version 5.6 (March 2018)
	Last major release	FCRM Version 5.6 (March 2018)
	Target market	Regional and global financial services companies

Source: Fiserv RFI

OVERALL FUNCTIONALITY

Figure 5: Functionality

SUITE FUNCTIONALITY	FEATURES AND FUNCTIONS		
Transaction Monitoring	See Celent report, Solutions for Anti-Money Laundering: 2018 Transaction Monitoring ABCD Vendor View		
Watchlist Screening	Real-time sanctions dispositioning	Real-time domestic payments dispositioning	Screening support for double-byte scripts
	Screening of external data sources	Automated download of watchlists	Automated delta updates
	Data cleansing / deduping	White list management	Support for internal lists
Onboarding / Customer Due Diligence	Risk scoring for onboarding	Risk scoring for customer review	Account opening checklist workflow
	STP integration with account opening systems	STP integration with core systems	STP integration with TM systems
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
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	

Yes – integrated into the AML platform
Yes – separate module offered by this vendor
Yes – through a formal partnership with another vendor
Not provided

Supported and already in production
Supported but not in production
Available through a 3rd party
Not supported

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 watchlist screening solution can be used to screen transactions, customers, policyholders, beneficiaries, and accounts. Screening can be performed in batch, on demand, or in real-time.

AML Risk Manager supports dynamic risk management, wherein customer risk scores created during the KYC process can be passed to the transaction monitoring module and, conversely, monitoring or screening results can be used to update the customer risk score.

The solution provides visualization tools such as depiction of beneficial ownership shares in an entity and map view of wire destination countries.

Fiserv's watchlist screening solution supports more than 10 official watchlists, including OFAC, OSFI, EU, HM Treasury, CIA Heads of State, and UN. The solution also supports FinCEN 314(a) requests. Commercial datasets supported include Accuity, Dow Jones Watchlist, LexisNexis, and Thomson Reuters.

The vendor states that 25% of its on-premise clients use the solution in multiple countries, including 30 clients using it in 5 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.

Items on the roadmap for Fiserv include beneficial ownership visualization; collection, scoring, and display of due diligence information; enhancements to the user interface, menus, and case management; and extended reporting.

RULES AND ANALYTICS

The AML Risk Manager watchlist screening product has a library of more than 70 preprogrammed matching algorithms that analyze a variety of source data elements against watchlists. Data elements can include account, customer (individual or entity), DoB, counterparty bank, counterparty beneficiary, and MT and ACH messages including narrative fields. The solution also allows for configuration of parameters such as alert thresholds and weighting of specific data fields. Users can select the match method used at the data field level. The solution also generates separate match scores for the various fields.

FALSE POSITIVES MANAGEMENT

According to Fiserv, AML Risk Manager achieves false positive rates ranging between 1% and 20%. Technology features designed to reduce false positives include screening of multiple fields; configuration of the algorithms used; exclusion of noise words; and white lists. The solution provides delta updates for both the source data and watchlist data in order to support more efficient screening routines. Rules to govern contextual screening are another method used by the solution to reduce false positives; an example is excluding vessel names when screening retail banking customers.

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 in order to support the fine-tuning of scenarios.

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	OFAC Annual Report of Blocked Parties, OFAC Transaction Report, goAML CRS, FATCA
REPORT AUTO-GENERATION, PDF	OFAC Transaction Report
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 are 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, Arabic, Dutch, French, Portuguese, Polish, Russian, Spanish, Vietnamese, and simplified Chinese.

CUSTOMER BASE

Fiserv has 1,140 clients worldwide in production with their watchlist screening system. The breakdown by financial sector, tier, and geography is given in the table below.

Table 7: Client Breakdown

SECTOR		TIER		REGION	
Retail/corporate banks	91%	Tier 1	3%	US/Canada	86%
Investment banks	3%	Tier 2	5%	Latin America	1%
Asset managers	1%	Tier 3	9%	Asia	3%
Insurers	3%	Tier 4	8%	Europe	7%
Other firms	2%	Tier 5	75%	Middle East	2%
				Africa	1%
				Rest of World	0%

Source: Fiserv RFI

Ninety-five percent of Fiserv's watchlist screening clients also use the vendor's transaction monitoring module. Eighty percent of Fiserv's watchlist screening clients also use the vendor's case management module. Seventy-five percent 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

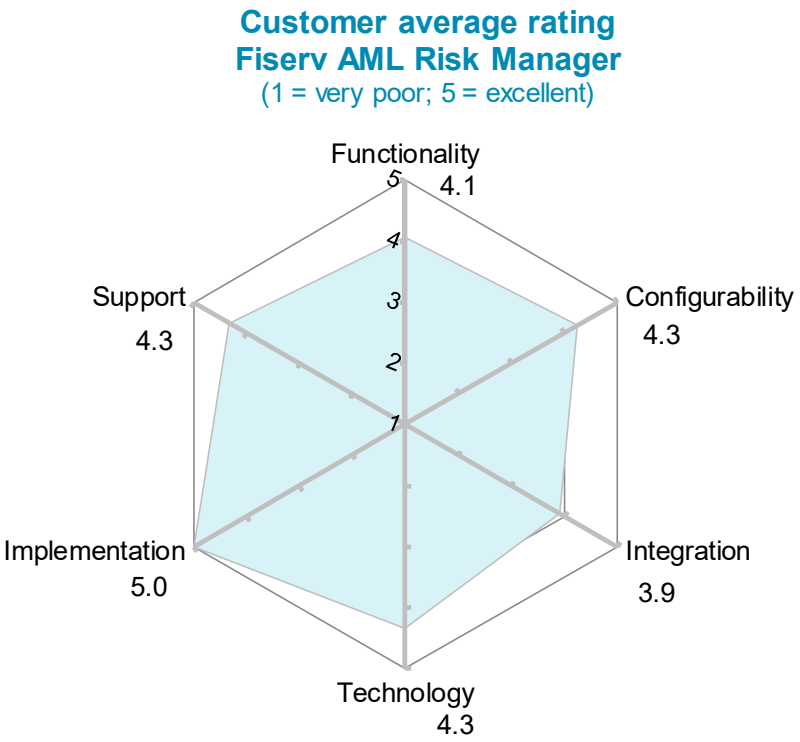
DEPLOYMENT CATEGORY	NUMBER OF CLIENTS
IN PRODUCTION WITH RELEASE OF LAST MAJOR CHANGE	1,140
IMPLEMENTING RELEASE OF LAST MAJOR CHANGE	140
IN PRODUCTION WITH PRIOR RELEASE	1,000
NEW CLIENTS SINCE 2014	270
DEPLOYMENT METHOD (PERCENTAGE OF CLIENT BASE)	On Premise: 40% Off-premise (hosted, SaaS, cloud): 60%

Source: Fiserv RFI

CUSTOMER FEEDBACK

Three clients provided feedback on Fiserv. Two are tier 3 clients, and one is a tier 1 client. Two use the system for retail and corporate banking, all three use it for asset management, one uses it for investment banking / brokerage, one for insurance, and one for credit cards. All three respondents use the solution in the US and/or Canada. All three clients have used the system for more than three years.

Figure 6: Customer Feedback



Source: 2018 Celent AML Watchlist Screening customer feedback survey. N = 3

Clients rated Fiserv strongly overall. In the area of functionality, clients liked the screening for KYC/CDD; while screening of adverse news, social data, and other unstructured data sources was seen as an area needing relative improvement. In terms of usability (configurability), user management (permissions, authority) and making minor changes were highlighted; while reports (design and maintenance) was an area of relative weakness. Within technology, ease of system maintenance was scored the highest, and flexibility of the data model was seen as somewhat weaker.

Clients felt the solution integrated most easily with external data sources and integrated less well with their onboarding and account opening systems.

Regarding their implementation experience, clients rated Fiserv highly across all areas in this category. Finally, in the area of ongoing system support, project management (estimations, scope creep, etc.) and work completed on budget received the highest scores; while speed of issue resolution and work completed on time were seen as areas of relative weakness.

Clients said the two or three best things about the vendor were workflow and case management, availability of list record information, user friendliness and simplicity of operation, holistic view, and ease of integration with Fiserv FCRM transaction monitoring. They suggested improvements for system speed, system upgrades, negative news screening capability, and the system's capacity for attaching additional documentation to client records and alert dispositions.

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); 100% Browser-Based (HTML with Flash, Silverlight or similar) Developers: 100% Browser-Based (HTML 5); 100% Browser-Based (HTML with Flash, Silverlight or similar)
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 watchlist screening engine is shown in the table 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 watchlist screening engine include: structured data; unstructured data – text; unstructured data – audio (via third party tools); and unstructured data - image/video (via third party tools).

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 watchlist screening solution are shown in the table below. There is no preference for 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 watchlist screening 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 watchlist screening 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 watchlist screening 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 a watchlist screening 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 configuration environments 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 in [list several here]. 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

Combatting Financial Crime at Scale with a Coordinated, Intelligent, Real-Time Response
October 2018

Enhancing AML Efficiency and Effectiveness: Artificial Intelligence Transforms the Rules of the Game
October 2018

Fighting Financial Crime Amidst Growing Complexity: The Need to Rethink AML Technology and Approach
October 2018

Solutions for Anti-Money Laundering: 2018 Transaction Monitoring ABCD Vendor View
September 2018

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

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

Achieving Holistic AML: Focus on Watchlist Screening
March 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.

Copyright © 2018 Celent, a division of Oliver Wyman, Inc., which is a wholly owned subsidiary of Marsh & McLennan Companies [NYSE: MMC]. All rights reserved. This report may not be reproduced, copied or redistributed, in whole or in part, in any form or by any means, without the written permission of Celent, a division of Oliver Wyman ("Celent") and Celent accepts no liability whatsoever for the actions of third parties in this respect. Celent and any third party content providers whose content is included in this report are the sole copyright owners of the content in this report. Any third party content in this report has been included by Celent with the permission of the relevant content owner. Any use of this report by any third party is strictly prohibited without a license expressly granted by Celent. Any use of third party content included in this report is strictly prohibited without the express permission of the relevant content owner This report is not intended for general circulation, nor is it to be used, reproduced, copied, quoted or distributed by third parties for any purpose other than those that may be set forth herein without the prior written permission of Celent. Neither all nor any part of the contents of this report, or any opinions expressed herein, shall be disseminated to the public through advertising media, public relations, news media, sales media, mail, direct transmittal, or any other public means of communications, without the prior written consent of Celent. Any violation of Celent's rights in this report will be enforced to the fullest extent of the law, including the pursuit of monetary damages and injunctive relief in the event of any breach of the foregoing restrictions.

This report is not a substitute for tailored professional advice on how a specific financial institution should execute its strategy. This report is not investment advice and should not be relied on for such advice or as a substitute for consultation with professional accountants, tax, legal or financial advisers. Celent has made every effort to use reliable, up-to-date and comprehensive information and analysis, but all information is provided without warranty of any kind, express or implied. Information furnished by others, upon which all or portions of this report are based, is believed to be reliable but has not been verified, and no warranty is given as to the accuracy of such information. Public information and industry and statistical data, are from sources we deem to be reliable; however, we make no representation as to the accuracy or completeness of such information and have accepted the information without further verification.

Celent disclaims any responsibility to update the information or conclusions in this report. Celent accepts no liability for any loss arising from any action taken or refrained from as a result of information contained in this report or any reports or sources of information referred to herein, or for any consequential, special or similar damages even if advised of the possibility of such damages.

There are no third party beneficiaries with respect to this report, and we accept no liability to any third party. The opinions expressed herein are valid only for the purpose stated herein and as of the date of this report.

No responsibility is taken for changes in market conditions or laws or regulations and no obligation is assumed to revise this report to reflect changes, events or conditions, which occur subsequent to the date hereof.

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