CELENT

CELENT
Awards 2023

FINANCIAL CRIME COMPLIANCE TECHNOLOGY: AML TRANSACTION MONITORING EDITION

2023 XCelent Awards, Powered by VendorMatch

Neil Katkov and Ian Watson

July 18, 2023

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

CONTENTS

Executive Summary **3**

Transaction Monitoring Market Overview **7**

Celent's ABC Vendor View **12**

AML Solutions: Definition and Functionality **13**

Vendor Profiles **22**

NICE Actimize: Suspicious Activity Monitoring Solution (SAM) 23

Path Forward **34**

For Financial Institutions 34

For Vendors 35

Appendix: Celent's ABC Methodology **36**

Leveraging Celent's Expertise **42**

Support for Financial Institutions 42

Support for Vendors 42

Related Celent Research **43**

© CELENT

EXECUTIVE SUMMARY

This is Celent's fifth review of anti-money laundering (AML) transaction monitoring systems available to financial institutions and other regulated companies. The 17 vendors profiled in the report—including both incumbent providers and new regtech entrants—show how next-generation technologies continue to reshape financial crime compliance in the financial industry.

Digital transformation in financial crime compliance has evolved through three technology pivots: machine learning (ML), digital tools such as no code configuration and process automation, and—most recently—large language models (LLMs). These technologies are becoming necessary capabilities for AML systems. Because they are still maturing, there remains ample opportunity within banks to realize more effective and efficient financial crime compliance operations by applying these and other next-generation techniques. How banks are doing this often depends on their size and position in the industry.

- Large financial institutions seeking to achieve these capabilities often continue to rely on incumbent financial crime compliance technology providers. Because incumbent systems typically suffer from high false positive rates due to a reliance on traditional rules, large institutions are supplementing these primary systems with AI-enabled solutions, as well as internal machine learning models. Some forward-looking institutions are even moving to an ML platform as their primary transaction monitoring solution.
- Smaller institutions, challenger banks, and non-bank sectors such as digital payments, crypto business, and gaming—which run on cloud-based, AI-enabled technology themselves—tend to choose digitally-enabled systems from new regtech entrants.
- At the same time, increasing regulatory focus on non-bank sectors is leading the non-banks to adopt incumbent solutions with stronger case management, compliance, and audit capabilities.

This report aims to support financial institutions with their financial crime compliance technology decisions. The report looks at both incumbent and regtech AML transaction monitoring systems from across the globe and evaluates them according to Celent's ABC Vendor View and Celent's Technology Capabilities Matrix.

The report features 17 profiled vendors and 12 fully participating in the ABC Vendor View analysis.

Celent's Technology Capabilities Matrix (TCM) offers a categorization of vendors and also includes vendors that did not participate fully in our ABC analysis. Celent's TCM assignments are shown in Figure 1 below.

Figure 1: Technology Capabilities Matrix: AML Transaction Monitoring

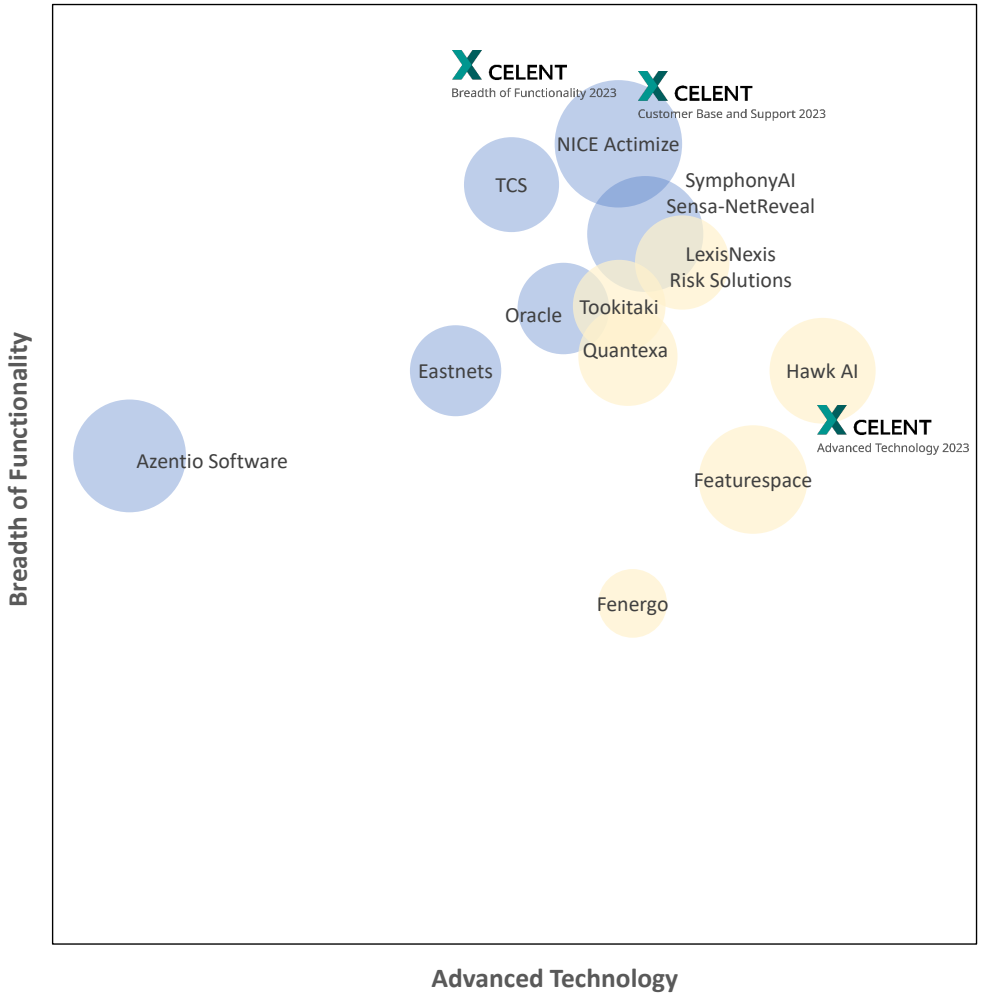


Source: Celent

Celent's ABC Vendor View analysis of AML Transaction Monitoring systems is shown in Figure 2 below. The top performers in each ABC dimension receive a corresponding XCelent Award. The winners of the XCelent 2023 Awards for AML Transaction Monitoring Systems are:

- XCELENT Advanced Technology 2023: **Vendor 5**
- XCELENT Breadth of Functionality 2023 : **NICE Actimize**
- XCELENT Customer Base and Support 2023 : **NICE Actimize**

Figure 2: Celent ABC Vendor View: AML Transaction Monitoring Systems



Relative size of bubble = Customer Base and Support. Key: = Incumbent solutions = New Entrants
Source: Vendor RFIs, Celent analysis

Financial Crime Compliance Report Series

Companion reports in Celent's 2023 series on AML systems will include:

- *Financial Crime Compliance Systems: Watchlist Screening Edition—2023 XCelent Awards, Powered by VendorMatch*: Evaluates providers of watchlist screening software.
- *Crypto Investigative Tools for AML: A Regtech Solutionscape*: Profiles providers of specialist AML solutions for cryptocurrencies,

TRANSACTION MONITORING MARKET OVERVIEW

This is Celent's fifth review of transaction monitoring systems for the anti- money laundering use case. The 17 vendors profiled in the report—including both incumbent providers and new regtech entrants—show how next-generation technologies continue to reshape AML operations in the financial industry.

Cloud delivery and artificial intelligence (AI), trends that were emerging in our last edition in 2018, are now becoming table stakes for financial crime compliance systems. Moreover, the supplier landscape has expanded dramatically with the addition of numerous new entrants offering digitally-enabled solutions. In turn, the incumbent providers of AML systems have been enhancing their offerings with digital capabilities in order to support these evolving technology requirements.

As a result of these shifts in technology and the supplier landscape, more than half of the systems profiled in this report were developed by new entrants over the past five to ten years. Most of the systems featured in this edition, whether new entrant or incumbent, offer cloud deployment options; all of the solutions incorporate some degree of AI functionality.

Financial Crime Compliance Technology: Three Pivots to Digital

The ongoing transition to AI-enabled, high performance financial crime compliance systems is a leading indicator of the application of digital technologies to risk functions at financial institutions.[1] Digital transformation in financial crime compliance has involved three groups of technologies: machine learning, digital tools, and, most recently, large language models (LLMs).

Regtechs were early adopters of machine learning for anti-financial crime, but the established players are quickly following suit. With virtually every AML vendor—incumbent or new entrant—now providing some degree of these capabilities, AI and machine learning have become table stakes in the AML space.

The COVID-19 pandemic was a turning point for the adoption of digital technologies for anti-financial crime. The pandemic unleashed a surge in financial crime activity. At precisely the same time, shelter-in-place restrictions resulted in seismic shifts in consumer behavior that challenged incumbent rules and models used in behavior

1. See Celent's report, *Digitizing the Risk Back Office: Five Themes for Risk in 2023*.

detection. As financial institutions worked overtime to update their existing models, the usefulness of AI for financial crime compliance came into sharper focus.

Table 1: Three Pivots To Digital in Financial Crime Compliance

Technology	Use Cases	Representative Vendors
Machine Learning	- False positives reduction - Anomaly detection	Featurespace, Google, SymphonyAI
Digital Tools	- No-code rules configuration - Process automation	Hawk AI, NICE Actimize, LexisNexis Risk Solutions
Large Language Models	- Assisted automation of alert/case investigation - Auto-generation of case narratives	Lucinity, Quantexa, SymphonyAI

Source: Celent

Machine learning quickly demonstrated its value by enabling significant reductions in the very high false positive rates of transaction monitoring and screening alerts that bedevil the industry. AI also provided new techniques for enhancing anomaly detection as opposed to traditional rules, although the early wins here were more in the anti-fraud space.

Meanwhile, digital tools to support flexibility and speed-to-market—including cloud-first technology architectures, process automation, and low code / no code configuration and rules testing—proved their value in supporting operational efficiency and regulatory change as the pandemic gave way to geopolitical and economic turbulence.

While some institutions are more active in technology transformation than others—including ABN AMRO, Societe Generale, and HSBC—these digital technologies are becoming necessary capabilities for AML systems. Because they are still maturing, there remains ample opportunity within banks to realize more effective and efficient AML operations by applying next-generation techniques.

Large language models (LLMs), a form of generative AI, are the latest technology in the digital toolkit. LLMs are already powering analyst copilots from **Lucinity**, **Quantexa**, and **SymphonyAI** to help automate investigation and analysis of alerts and cases. Trained on internal and curated external data, LLMs are poised to contribute to virtually every task in case management and reporting workstreams.

AML Systems: The Supplier Landscape

Sourcing of AML systems falls into roughly four categories.

1. **Incumbent financial crime compliance specialists.** These are vendors that largely or exclusively focus on anti-financial crime solutions and have mature products with 20 to 30 years of experience in the space. Incumbents frequently provide solutions for AML, fraud, and, in some cases, trade surveillance, built on the

same core platform. The client base of these incumbents is dominated by mainstream financial institutions. However, as newly regulated segments such as digital payments, crypto business, and gaming develop greater needs for "bank-ready" compliance solutions they may turn to an incumbent provider to meet these needs. In response to customer requirements, the incumbent providers have introduced cloud deployment options, built out machine learning capabilities, and are incrementally moving their technology to API-enabled microservices architectures.

- Incumbents profiled in this report include **Eastnets**, the **NetReveal** solution of SymphonyAI (now being integrated with Sensa, SymphonyAI's regtech solution), **NICE Actimize**, **Oracle**, **SAS**, and **Verafin**.

2. **New regtech entrants.** This segment comprises providers of anti-financial crime solutions typically built on digital, cloud-first technology platforms and launched over the past 5 to 15 years. The client base of regtech providers is focused on digital businesses such as neobanks, fintechs, payment service providers (PSPs), ecommerce firms, crypto businesses, and gaming companies. Some regtechs offer enterprise-grade systems and have succeeded in selling to top tier financial institutions. Regtech solutions are typically built on highly scalable data and analytics platforms to support the real time, high volume requirements of digital businesses and to provide the high performance computing needed to power AI-based detection models.
   - New entrants profiled in this report include **Featurespace**, **Fenergo** (Sentinels acquisition), **Google Cloud**, **Hawk AI**, the RiskNarrative system of **LexisNexis Risk Solutions**, **Napier**, **Quantexa**, and **Tookitaki**.
3. **Financial services industry technology conglomerates.** This group of vendors provides financial institutions with a range of technology solutions, often with a strong focus on core banking and related systems. The AML systems offered by FSI conglomerates are but one part of a suite of interconnected systems. These systems were typically developed 20 to 30 years ago, positioning them as incumbents with established client bases.
   - FSI tech conglomerates profiled in this report include **Azentio**, **Kiya.ai**, and **TCS**.
4. **Internal build.** The ongoing digitization of anti-financial crime technology has eroded but not entirely erased build-versus-buy decisions at large financial institutions. As new regtech entrants led the charge in introducing AI and cloud-native high performance computing to AML systems, many large banks ran proof-of-concept (PoC) engagements or entered into strategic investments with these startups. While this led to some adoption of regtech AML solutions by these institutions, it also provided an opportunity for them to explore the potential of digital technologies to enhance AML operations. As a result, large institutions with internal data science capabilities may now opt to build next-generation capabilities themselves.

Demand Trends

Financial institutions are increasingly keen to adopt machine learning and other digital capabilities to enhance financial crime compliance operations. The technology choices to achieve this goal differ between large, established financial institutions on the one hand, and smaller institutions as well as non-bank financial services providers on the other.

Incumbents. The prevalent pattern at large institutions such as Tier 1 and Tier 2 banks is to keep their incumbent transaction monitoring systems—like **NetReveal** (now part of SymphonyAI), **NICE Actimize, Oracle**, or **SAS**—but supplement them with additional systems to provide digital capabilities. A number of large banks run a second or parallel pass on transactions through AI platforms such as **SymphonyAI Sensa**. **Quantexa**, which provides a graph analysis-based system, has been implemented by a number of large banks to support detection in specialized lines of business like trade finance and capital markets, as well as for enterprise-wide periodic monitoring. Some forward-looking institutions are even moving to an ML platform, such as **Featurespace** or **Google Cloud**, as their primary transaction monitoring solution.

Internal build. Large banks with internal data science capabilities are also developing and maintaining their own machine learning models that run on top of rules. This is primarily to reduce the high false positive rates of their incumbent transaction monitoring systems, but also for additional anomaly detection.

New entrants. Smaller institutions like challenger banks as well as non-bank regulated sectors such as payments, crypto business, and gaming, have been active in choosing regtech entrants like **ComplyAdvantage**, **Hawk AI**, the RiskNarrative product of **LexisNexis Risk Solutions**, **Napier**, and **Tookitaki**. New companies in these sectors typically run on cloud-based, AI-enabled technology themselves, making digitally-enabled compliance solutions a close fit. Large banks may also implement regtech AML solutions in specialized lines of business such as private banking or insurance.

These demand trends are reflected in the client base of the solutions profiled in this report.

Clear Trajectory Toward Machine Learning

Celent expects adoption of machine learning solutions by mainstream financial institutions to continue as barriers to implementation decrease. Internal data science initiatives are providing teams with proficiency in machine learning and leading to improved governance processes around model management. Implementations of digitally-enabled solutions for specific lines of business or to augment incumbent financial crime compliance systems are also providing a training ground as well as proof points for the efficacy of machine learning and other digital tools.

HSBC is a good example of the trend to digital transformation in financial crime compliance. HSBC runs AML for its insurance line of business on **Featurespace**, a cloud-based, AI-enabled transaction monitoring platform. HSBC also uses **Quantexa** across its entire global footprint to support risk detection through network analytics.

Most recently, HSBC has implemented the new cloud-based transaction monitoring system from **Google Cloud**, which runs machine learning models exclusively.[2] HSBC intends to deploy the system globally as its primary AML system. This is a sign of things to come in the overall transition of risk functions to a digital footing, as well as an indication that the financial crime compliance space is starting to attract technology heavyweights like Google.

Large Language Models

Large language models are a form of text-based generative AI that have the ability to significantly increase productivity in compliance workflows through chatbot-based human-machine collaboration. Initial use cases for LLMs in financial crime compliance, and more specifically transaction monitoring, focus on assisting analysts at the alert and case management stage by performing routine investigation tasks. LLMs trained on internal and curated external data can also be used to write explanatory summaries of case summaries and SAR narratives for filing with regulators. **Lucinity** and **SymphonyAI** have already launched LLM-based analyst copilots of this sort, and **Quantexa** is developing one. LLMs to support specialized use cases such as document-heavy trade finance are likely on the horizon. An emerging technology, LLMs will have to clear reliability, bias, and regulatory issues before they are widely adopted. Celent believes that LLMs and generative AI will quickly become an important differentiator in the financial crime compliance space.

[2] See Celent's report, *HSBC: Cloud-Based Financial Crime Detection at Scale*.

CELENT'S ABC VENDOR VIEW

To help financial institutions better understand the vendor landscape and compare providers, Celent developed its ABC methodology, which positions vendors across three dimensions: **A**dvanced Technology, **B**readth of Functionality, and **C**ustomer Base and Support.

The final rating for each of these three dimensions is based on 1) vendor responses to a Celent RFI, 2) product demonstrations to Celent analysts, and 3) client responses to a customer reference survey. The final rating is determined by Celent's score of these factors as well as our view of the relative importance of the factors as they apply to both solution and vendor capabilities. The latter determines the weight Celent places on each variable.

This report normalizes all scores on a 0 to 10-point scale. As a result, we are able to show relative scores for each ABC edition in the financial crime compliance space and, importantly, help financial institutions differentiate vendors across their peer group.

Celent invited 40 vendors of AML transaction monitoring software worldwide to participate in Celent's research. Because some vendors chose not to participate or ultimately did not fulfill the participation requirements, the final report features 14 fully profiled vendors and 12 participating in our ABC Vendor View analysis. Celent's ABC Methodology is described in detail in the Appendix. The report also features three brief profiles on vendors that for various reasons did not participate in the RFI.

We suggest 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 goals and solution requirements.

© CELENT

AML SOLUTIONS: DEFINITION AND FUNCTIONALITY

Anti-money laundering systems support financial crime compliance operations at banks, insurers, securities and investment firms, and other financial institutions; as well as regulated companies including fintechs, payment service providers, cryptocurrency businesses, and gaming companies.

While there is a continuing trend among vendors toward offering a suite of solutions providing end-to-end financial crime compliance functionality, some vendors focus on a subset of the AML value chain, such as watchlist screening, KYC, or transaction monitoring. 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. Smaller financial institutions and non-financial regulated companies tend to go with one provider, while large firms invariably have complex and siloed operations that leverage systems from multiple vendors.

Definition

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

AML Suite Capabilities

Celent categorizes anti-money laundering solutions into five suite-level categories. These categories correspond to the basic modules offered by many vendors. Among these five categories, this report evaluates the AML transaction monitoring (TM) or behavior detection capabilities of financial crime compliance software vendors, as well as associated case management and reporting features.

© CELENT

Figure 3: AML Software Suite Categories



Source: Celent
= Categories covered in this report.

The five categories are:

1. **Know Your Customer (KYC).** Onboarding and customer due diligence (CDD) are essential KYC processes that leverage watchlist screening, workflow for collecting customer documents and information, and risk scoring to create risk profiles of prospective, new, and existing customers. Customer information, risk scores, and expected account activity may also be accessed by TM engines as a parameter for behavior analysis.

2. **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.

3. **Transaction monitoring.** Transaction monitoring refers to the periodic or real-time analysis of financial and nonfinancial transactions to identify unusual account or customer activity that may indicate financial crimes such as money laundering, fraud, market abuse, or trade misconduct. TM software employs SQL query-based rules, machine learning models, or a combination of both to identify unusual transactions or sequences of transactions. The TM engine generates exceptions (“alerts”) for activity meeting the rules or model criteria; many systems will also assign a risk score to the exception indicating the severity of the activity and list the specific rules or activity 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.

4. **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 workflows; interactive screens with data sorting and drilldown; and visualization tools such as risk analysis charting and network and flow-of-funds visualization (network 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. An emerging capability is the use of natural language generation (NLG) or LLMs to auto-create alert summaries and SARs narratives.

   In some cases, financial institutions do not use the case management module of their TM or WL vendor; instead, they 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.

5. **Reporting.** The reporting functionality of an AML system includes support for regulatory reports along with 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. US FinCEN and the UN's goAML report format, currently used in some 50 countries, are two reporting formats frequently required by financial institutions.

   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 business intelligence visualization software such as Tableau; and third party reporting tools like SAP Crystal Reports, particularly for custom reports.

Some vendors offer additional capabilities by means of modules. Examples include modules for forensic investigation, business intelligence-based visual reporting, graph analysis, scenario tuning/segmentation, and AI modeling tools. This report discusses such capabilities under the appropriate suite-level category.

A companion report, *Financial Crime Compliance Technology: Watchlist Screening Edition—2023 XCelent Awards, Powered by VendorMatch* evaluates transaction and customer screening systems.

Transaction Monitoring: Key Features

The table below displays some of the specific features used to evaluate AML transaction monitoring systems in this report. A color-coded version of these features appears in the Vendor Profiles to indicate each solution's support for each function. Additional characteristics of the systems are presented in tables and discussed in the system profiles in this report.

Table 2: Transaction Monitoring Systems: Key Features

Function	Features	Function	Features
Behavior Detection	Real Time Monitoring	**Case Management**	Workflow Configurability
	Monitors All Transactions		Process Automation
	Historical Profiling		Entity-Based Alerts
	Product/Transaction Support		Investigations Support
	Language/Currency Support		Visualization Tools
	Channel Support		AML/Fraud Integration
Rules and Analytics	Pre-packaged Rules		Assignments/Queueing
	Rules Configuration	**Reporting**	Prepackaged Reports
	AI/Machine Learning		Ad Hoc Reporting
	Risk Scoring		Regulatory Reporting
	Network/Link Analysis		Audit Trail
	False Positives Reduction		

Source: Celent

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

Behavior Detection Features

Real time monitoring. 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 in AML. The convergence of AML and fraud may also be a factor in moving AML to a real time paradigm.

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. More sophisticated 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 behavior of all customers with similar characteristics. 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.

Some solutions apply AI techniques to profiling to enrich the analysis with additional features or to identify when atypical activity is likely to be licit behavior (as a false positives reduction technique).

Language/currency support. 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.

Rules and Analytics

The types of rules, scenarios, and AI models available, and the tools provided to manage them, are an important differentiator for AML transaction monitoring systems.

Prepackaged rules. Rules interrogate source databases for financial or nonfinancial transactions that meet 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 in assessing the libraries of preconfigured rules provided by vendors.

Typologies. Some vendors provide more sophisticated models for detecting specific financial crime typologies. These models combine traditional volume-and-velocity type rules with other properties, such as business type or geographic risk. They may also use AI or natural language processing (NLP) to detect specific patterns or

characteristics associated with typologies. Typology libraries are often designed to detect the money laundering typologies disseminated by the Financial Action Task Force (FATF) and other regulatory and quasi-regulatory bodies.

Rules configuration. An important consideration for firms that develop rules in-house 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 into 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. Newer solutions that support real time monitoring often incorporate a sandbox within the production environment to support rules testing and deployment during runtime.

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.

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 at the preprocessing (pre-alert) stage include rules tuning and segmentation. Post-processing techniques to reduce false positives reduction include prioritization and triage based on risk scores and alert suppression using whitelists. Many vendors are applying AI and machine learning techniques to the false positives challenge, such as suppressing alerts that exhibit similar properties to previous alerts that were determined by analysts to be false positives.

Network/link analysis. At its most basic, network analysis displays transaction flows between accounts. These links or networks may be displayed to compliance analysts in graphic form or as tabular information. The analysis may also show various relationships and commonalities between accounts, including common account holder, beneficial owner, address, business, or external counterparty, among other characteristics. Advanced network analysis uses knowledge graph and AI techniques, supplemented by domain expertise in money laundering typologies, to optimize the detection and interpretation of common elements in the data, and to generate and score actionable alerts on specific entity and activity patterns. Network analysis at this level can be used to supplement or replace traditional monitoring engines.

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, post-processing rules and analytics, and process automation features 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 low code / no code 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. Robotic process automation (RPA) and machine learning are important techniques offered by some vendors for automating aspects of case management workflow.

Visualization tools. 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 such as corporate data and adverse media.

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.

Integration with third party transaction monitoring systems. The capacity to export or import transaction flows from a third party TM system may be an important consideration for firms that wish to apply additional detection analytics. Similarly, the ability to export alerts to third party case management systems can support the consolidation of output from multiple monitoring systems into one alert/case investigation stream, or support firms taking a best-of-breed approach to selecting their case management module or that use a proprietary system. Bidirectional APIs provide a flexible, agile approach to integrating transaction flows, alerts, or other data.

AML/fraud integration. 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 to 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.

Assignments/queueing. Automated assignment of alerts and cases to available analysts, including alert and case queueing, 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.

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, natural language generation, and now large language models are 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, a complete record of analyst actions on the one hand and a detailed log of system modifications on the other are important to support best practices in internal employee and IT governance, external audit, and regulatory compliance.

Digital Technology Capabilities

The AML technology space has evolved rapidly over the past five years, with advanced technologies including AI/machine learning, RPA, and NLP/NLG all being deployed in efforts to optimize AML compliance operations. The profiles in this report point out the uses of these technologies by both incumbent AML solution vendors and new entrants.

AI/machine learning. Machine learning was first applied to the AML behavior detection use case nearly two decades ago, pioneered by **Verafin** and others. Today, AI capabilities are available through standalone AI platforms tailored for anti-financial crime detection and as a value-added feature in more productized transaction monitoring systems that use a hybrid AI/rules approach to transaction monitoring. AI platforms support a wide variety of supervised, unsupervised, and deep learning techniques to optimize detection of both known typologies and anomalies. AI is often used in productized TM systems to enhance anomaly detection and to target specific requirements such as alert prioritization, false positives reduction, or network analysis. AI platforms and some productized systems support the importation of AI models developed by internal data science teams or by third party providers, as well as the development and maintenance of AI models within the solution itself.

Unstructured data analysis. AML transaction monitoring primarily involves analysis of financial and nonfinancial transaction data resident in core systems, customer information files, and other structured data sources. Even some AI platforms are only capable of structured data analysis. 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 knowledge-graph based analytic techniques are all driving increased interest in unstructured data analysis within transaction monitoring. Unstructured data analysis can also support enriching alerts with rich data such as analyzed and curated adverse media, beneficial owner information, and network analysis.

Cloud-first solution architecture. As more financial institutions move AML workloads to the cloud, support for cloud deployment is becoming a table stakes requirement for AML systems. Some incumbent vendors provide the option of deploying their existing solution in a private or public cloud environment. This approach affords some flexibility in deployment, but limited cost efficiencies.

New regtech entrants typically offer cloud-native solutions that support multitenancy, are built on a microservices architecture, are highly exposed through bidirectional APIs to support speedy and seamless integration with other systems, and are developed on an agile, continuous delivery basis. This SaaS-based approach to cloud deployment minimizes the cost of deployment and maximizes the speed-to-market of new features. Cloud-native technology also gives these solutions access to the development tools, high performance compute, and scalable data storage—capabilities needed to power AI models—that are offered by commercial cloud providers such as **AWS**, **Google**, and **Microsoft Azure**. Some incumbent providers are modernizing their cloud-based offerings by incrementally moving them to microservices, API-enabled architectures.

VENDOR PROFILES

The following sections profile each of the 17 AML transaction monitoring vendors and their solutions. The 14 full profiles include a company overview, product overview, product analysis, recent and planned product enhancements, selling and servicing, and Celent's assessment of the company/product. All vendor-supplied information cited in the following profiles was accurate as of May 2023.

The table below lists the vendors profiled in this report, along with their regional client footprint. Vendors fully participating with detailed RFI responses and customer references are included in the ABC Vendor View and the Technology Capabilities Matrix. Those who provided RFI details but not customer references have Vendor Profiles without Customer Feedback and are included in the Technology Capabilities Matrix only. Vendors had an opportunity to review their profiles in this report for factual accuracy. Some of the vendors profiled are Celent clients, and some are not. We present vendor information objectively, regardless of commercial relationship.

Table 3: List of Profiled Vendors

	NA	EMEA	APAC	LATAM	ABC
System 1	■■	■■	■■	—	✓
System 2	—	■■	■■	—	✓
System 3	■■	■■	■	—	✓
System 4	■■	■■	—	■	✓
System 5	■■	■■	■	■	✓
System 6	—	■	■	■	
System 7	■	■■	■■	—	
System 8	Data not provided by vendor				✓
System 9	Data not provided by vendor				
NICE Actimize	■■	■■	■■	■■	✓
System 11	Data not provided by vendor				✓
System 12	Data not provided by vendor				✓
System 13	Data not provided by vendor				✓
System 14	■■	■■	■■	■■	
System 15	■■	■■	■■	—	✓
System 16	Data not provided by vendor				✓
System 17	■■	—	—	—	

Key: ■■ = 3 or more clients in production in regions; ■ = 1–2 clients; — = Not in region

Source: Vendor RFIs, Celent analysis

NICE ACTIMIZE: SUSPICIOUS ACTIVITY MONITORING SOLUTION (SAM)

Company and Product Snapshot

Actimize, founded in 1999 and acquired by NICE in 2007, provides financial crime compliance software applications covering anti-money laundering, anti-fraud, and financial markets compliance. The Actimize division accounted for some 18% of NICE's revenues in 2021.

Table 4: Company Snapshot: NICE Actimize

Year Founded	1999
Headquarters	Hoboken, New Jersey, USA Corporate HQ: Ra'anana, Israel
Number of Employees	7,900+
Revenues (USD)	US$2.2 billion
Financial Structure	Public company NASDAQ: NICE
VendorMatch Link	https://www.celent.com/vendormatch/discovery/vendors/318493059

Source: Vendor RFI

The NICE Actimize Suspicious Activity Monitoring (SAM) Solution AML transaction monitoring solution was first released in 2005/2006 and is currently on version 9.2. The last major change to the technology base of the solution was in 2018; that release included machine learning and RPA capabilities.

Table 5: Product Snapshot

Name	NICE Actimize Suspicious Activity Monitoring (SAM) Solution
Year originally released/In Production	2005/2006
Current Release (Date of Release)	SAM 10.1 (2023)
Revenue Derived from the Product	NICE does not provide annual revenue for individual products
R&D Expense	About 15 percent of revenue
FTEs Providing Professional Services for Product	409
Notable Clients	Desjardins; LGT; Rakuten

Source: Vendor RFI

Celent Opinion

NICE Actimize's AML transaction monitoring system is a comprehensive solution with strong behavior detection, case management and reporting capabilities. The solution incorporates machine learning-based predictive scoring and entity resolution to reduce false positives, consolidate alerts, and support entity risk assessment.

- NICE Actimize's case management supports integrated investigation of alerts by bringing together a variety of data such as current and previous TM alerts as well as adverse media screening results—via its DataIQ KYC screening solution—for the alerted entity, beneficial owners, and counterparties.
  - Case management features a network analysis tool that enables interactive investigation of account relationships and funds flows based on this integrated data.
- NICE Actimize supports financial crime behavior detection for crypto assets by combining risk data from CipherTrace with analysis of the client's internal transaction records through SAM to generate alerts on crypto activity.
- NICE Actimize's X-Sight Marketplace is a curated ecosystem of 75+ application, data and tool providers supporting financial crime compliance, many of which can be integrated with Actimize solutions.

SAM's large customer base is dominated by banks, as well as clients across the financial services. Actimize also provides the solution to digital businesses seeking to strengthen their back-office AML operations with a "bank-ready" solution, particularly in North America. NICE Actimize is also seeing rapid growth in cloud-based deployments of its solution.

Roadmap highlights for NICE Actimize's transaction monitoring solution include entity resolution for external counterparties; graph DB-based network analysis and graph DB-based detection scenarios to uncover organized criminal activity such as human trafficking, trade-based money laundering and money laundering through capital markets; shared AI model learning to enhance predefined rules; and alert-level simulation.

Table 6: Celent's View of NICE Actimize Suspicious Activity Monitoring (SAM) Solution

Strengths and Differentiators	Caution Points	Coolest Feature
• AI-based predictive scoring for prioritizing and hibernating alerts • Regulatory reporting support for multiple jurisdictions • Support for cloud-based deployment	• Does not support real time transaction monitoring	• Integrates data from multiple Actimize solutions to support investigations within case management

Source: Celent analysis

Functionality

Celent's assessment of the NICE Actimize system's functionality is shown below.

Table 7: AML Transaction Monitoring Features Availability

Function	Features	Availability
Behavior Detection	Real Time Monitoring	○
	Monitors All Transactions	●
	Historical profiling	●
	Product/Transaction Support	●
	Language/Currency Support	●
	Channel Support	◎
Analytics	Prepackaged Rules	282
	Rules Configuration	●
	Risk Scoring	●
	Network/Link Analysis	◎
	False Positives Reduction	◎
	AI/Machine Learning	⊙
Case Management	Workflow Configurability	◎
	Process Automation	◎
	Entity-Based Alerts	●
	Investigations Support	●
	Visualization Tools	●
	AML/Fraud Integration	●
	Assignments/Queueing	●
Reporting	Prepackaged Reports	●
	Ad Hoc Reporting	●
	Regulatory Reporting	●
	Audit Trail	●

●	All features supported	●	All features supported with integration to separate module from vendor
◎	Most features supported	◎	Most features supported with integration to separate module from vendor
⊙	Some features supported	●	All features supported, mix of out of the box and available with integration
◎	Few features supported	◎	Most features supported, mix of out of the box and available with integration
○	Not available	●	All features supported with 3rd party integration
		◎	Most features supported with 3rd party integration

Source: Vendor RFI

Analytics

The system's support for analytics is outlined in the table below. The solution comes with more than 280 predefined rules, including specific rules for retail and correspondent banking, securities, insurance, and other lines of business. Actimize also provides several "security blanket" rules for detecting anomalies.

Actimize leverages artificial intelligence (AI) in a variety of ways. Supervised learning is used to score and prioritize alerts and to detect anomalies. Unsupervised learning is used for entity resolution and for entity segmentation using clustering. The solution includes notebooks-based AI workflows to support these capabilities as well as tuning.

Table 8: Support for Analytics

Function	Availability
Alert Generation: Predefined Rules	✔
Alert Generation: Predictive Analytics	✔
Alert Generation: AI	✔
Network Analysis Visualization	✔
Unstructured Data Analysis	✔
Unstructured Data Analysis: Adverse Media	☐
Big Data Analysis	✔

Legend: ✔ = In production; ☐ = Supported but not in production; ✕ = Not supported

Source: Vendor RFI

According to the vendor, their solution achieves average false positive rates of 61–70%. Features used to reduce false positive rates for transaction monitoring include predictive scoring, based on a supervised continuous learning model and historical outcomes, to predict the likelihood an alert will result in a SAR. The model hibernates likely false positive alerts in line with the client's policies and threshold tolerance until and if their risk increases. According to the vendor, the predictive scoring mechanism has been shown to reduce alert volumes by 27% and to accurately predict SAR filing requirements for the riskiest 20% of alerts.

Automation

Process automation capabilities within case management include RPA for evidence gathering and entity enrichment tasks to replace repetitive manual efforts. The solution can ingest alerts generated by third party NLP providers.

Table 9: Support for Process Automation

Function	Availability
Entity-Based Alerting	✔
Auto-Creation of Cases: RPA	✔

Auto-Creation of Cases: NLP and NLG	☐
False Positives Suppression: Rules	✔
False Positives Suppression: ML	✔
Auto-Reporting: Templates	✔
Auto-Reporting: NLG	✔

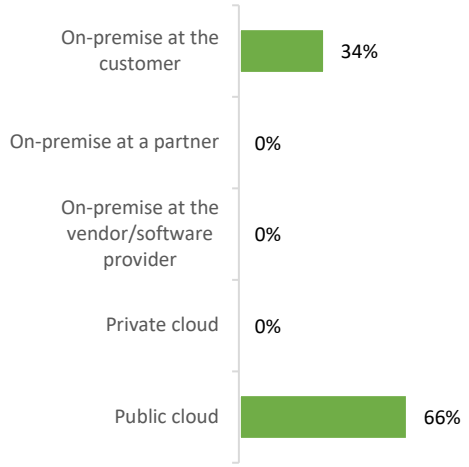
Legend: ✔ = In production; ☐ = Supported but not in production; ✕ = Not supported

Source: Vendor RFI

Customer Base

SAM has a total of 313 clients worldwide in production with their AML transaction monitoring system. A growing number of these clients deploy the system on the public cloud. The client roster is dominated by retail and corporate commercial banks. Clients also include sell side and buy side firms, insurers, money services businesses, e-commerce, gaming, and healthcare.

Figure 4: Client Base by Deployment Option



Source: Vendor RFI

Table 10: Industry Sectors Supported

Sector	Availability
Retail Banking	✔
Corporate Banking	✔
Brokerage	✔
Asset Management	✔
Hedge Funds	✔
Insurance	✔

Money Services Business	✔
E-commerce companies	✔
Casinos	✔
Non-financial corporates	✔

Legend: ✔ = In production; ☐ = Supported but not in production; ✕ = Not supported

Source: Vendor RFI

Actimize has implemented its AML transaction monitoring system in the countries shown in the table below.

Table 11: Implementations by Country

Region	Countries
North America	Canada, United States
Europe	Azerbaijan, Denmark, France, Germany, Greece, Hungary Ireland, Italy, Norway, Poland, Portugal, Spain, Sweden, Switzerland, United Kingdom, Turkey
Middle East	United Arab Emirates, Israel
Africa	South Africa, Nigeria
Asia-Pacific	Australia, Hong Kong, Japan, Singapore, South Korea, Taiwan
Central America	Costa Rica, Mexico, Nicaragua, Panama
South America	Bolivia, Brazil, Peru
Caribbean	-

Source: Vendor RFI

Customer Feedback

Three clients provided feedback on NICE Actimize. One client has operations in North America, EMEA, APAC, and LATAM; and two clients are based in North America. The system is deployed on-premise at all three clients. One client has been using the system for six years, another client has been using it for three to five years, and the last client is still implementing it.

Clients rated NICE Actimize strongly overall. For functionality, respondents appreciated the network/link analysis features, while process automation was not rated as favorably. Within technology, scalability of the solution was scored the highest and ease of system maintenance was seen as weaker.

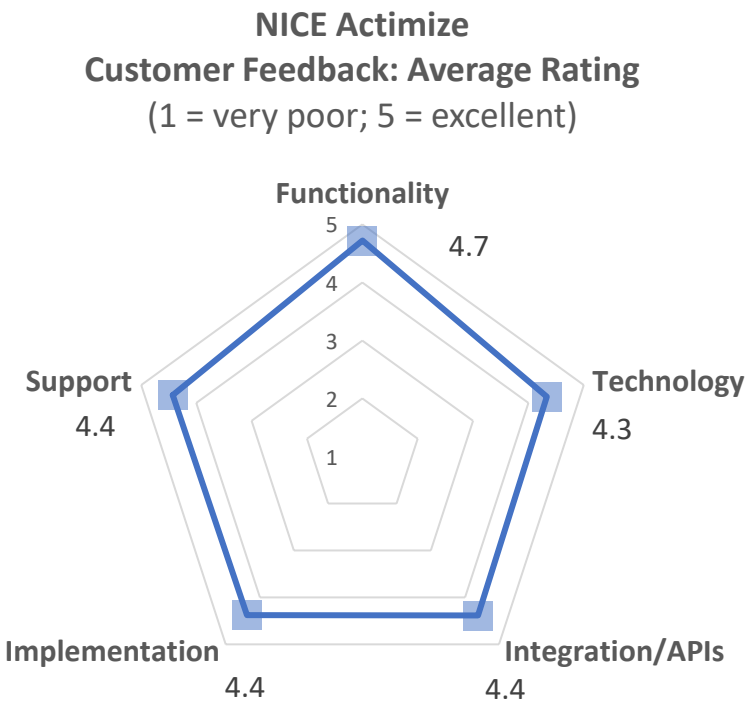
Clients felt the solution integrated most easily with their third party transaction monitoring systems and integrated less well with reporting systems. Regarding their implementation experience, the vendor's knowledge of their solution and relevant technology received the highest marks while project management (estimations, scope creep, etc.) received the lowest score. Finally, in the area of ongoing system support, responsiveness (handling and speed of issue resolution) received the

highest score while work completed on budget was seen as an area of relative weakness.

When asked what they liked best, one client appreciated the solution's ability to support the firm globally, the ease of version upgrades, and the centrality of support and maintenance services. Another client said the system was relatively easy to use for their operations team and has great capabilities. The last client appreciated that SAM is an industry-respected tool with broad support and usage; it benefits from continued development and releases to keep up with changing regulatory and AML regulatory trends. It's also highly configurable so the application can be tailored to the institution's needs.

Regarding suggested improvements, one client said no improvements were required. Another client suggested the product was US-centric and could use a more regionalized approach. The last client opined that the system's configurability comes with a downside: so much flexibility leads to significant complexity and the upgrade/change process can be difficult, time consuming, and expensive as a result.

Figure 5: Customer Feedback

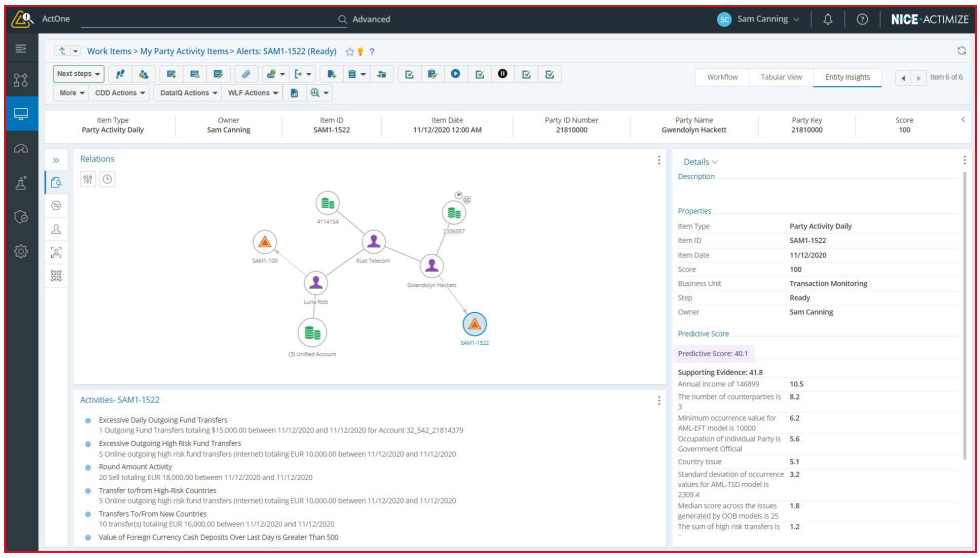


Source: Celent AML Transaction Monitoring Client Reference Survey

Technology

All of NICE Actimize's financial crime solutions are based on a common data model, which is made available to clients. The model includes customizable data fields which can be used to extend the model; this is done during implementation. Tables can be added to the model during implementation to support external data that is not supported by the standard data model. Each Actimize solution can use the system's APIs to transfer data to the other solutions.

Figure 6: Screenshot— NICE Actimize Suspicious Activity Monitoring (SAM) Solution



Source: Vendor

Table 12: Technology Options

Technology Options	Responses
Code Base	Java; Scala; JavaScript; Angular; PL/SQL; Actimize developed proprietary language for rapid model development; C++
Databases Supported	Oracle, SQL
Integration Methods	Web services; XML, not through web services; HTML; HTTP; RESTful HTTP-style services; JSON format; MQSeries, JMS or similar queue technology; Custom APIs; Flat files; Native messaging
Scalability	Largest live deployments: - 110 million transactions per day across 20 million active accounts. - 100,000 users; 1,000+ concurrent users
API Details	✓ The API is documented

Technology Options	Responses	
	✓	External systems can trigger an event in the system which can be responded to by a workflow or business rules system
	✓	API sample codes are available to clients
	✓	The system allows API publishing in SOAP, REST, JSON, and XML style services as APIs

Legend: ✔ = Available; ☐ = Not available

Source: Vendor RFI

Architecture and technology features that support SaaS deployment of the solution are outlined in the table below.

Table 13: SaaS Capabilities

Elements	Availability
Supports a multi-tenant architecture	✔
Type of effort required to update the solution	Automated scripts—fully automated
Cadence of upgrades for multi-tenant deployments	Every 3 months
Ability of the deployment model to leverage a serverless approach	✔
Proportion of the system architected as microservices	Over 80%
Supports automation of development and deployment processes (DevOps)	✔
Ability of the system's functions and capabilities to be distributed among a private cloud and a public cloud	✔

Legend: ✔ = Yes ✕ = No

Source: Vendor RFI

The table below shows which aspects of the solution can be configured by business and/or IT users and which aspects require vendor involvement.

The vendor estimates that, in recent implementations, 10% of total costs were the result of core code/development modifications.

Table 14: Change Tooling and Upgrades

Types of Changes	Availability
Business Rule Definition	✔
Data Definition	☐
Table Maintenance, List of Values, etc.	☐
Interface Definition	☐
Product Definition	✔
Role-Based Security, Access Control, and Authorizations	✔

Types of Changes	Availability
Screen Definition	☐
Workflow Definition	✔

Legend: ✔ = Configurable via tools for business users; ☐ = Configurable via tools for IT users; ■ = Configurable via the vendor; ⊖ = Configurable via scripting; ● = Coding required; ✕ = Not available

Source: Vendor RFI

Partnership

The vendor's implementation and functionality partners are shown in the table below.

Table 15: Implementation and Support

Type of Partnership	Partner Vendor
System Integrators	Infosys, TCS, IBM, Unisys, Matrix IFS
Fintech/Regtech Partners	Technology partnerships: Finastra, FIS, Datastax, AWS, Tableau, CipherTrace, Senzing 75+ partners in the Actimize X-Sight Marketplace, including CipherTrace (crypto AML) and Senzing (entity resolution)

Source: Vendor RFI

Implementation, Pricing, and Support

Support for implementation and service is indicated in the table below.

Table 16: Implementation, Support, and Pricing Models

Typical Implementation Team Size	6 to 10
Resource Breakdown	Vendor: 50%; Client: 50%; Third Party: 0%
Location of Employees	North America: 133, EMEA: 84, APAC: 192, LATAM: 0
Average Time to Implementation	Initial Implementation: 4 to 6 months 2nd and subsequent line of business: 1 to 3 months 2nd and subsequent states/jurisdictions: 1 to 3 months
Pricing Models	Subscription-based license, Term license, Perpetual license, Enterprise license
Annual Maintenance Fee	20%

Source: Vendor RFI

The total cost to implement this AML transaction monitoring solution can vary according to the scope of system use and other factors. The table below provides some typical costs for licensing, implementation fees and other out-of-pocket costs

paid to the vendor, and other costs (third party vendors/contractors, hardware, etc.) for the first year and subsequent years.

Table 17: Implementation and Running Cost Estimates

	Licensing	Implementation/ Vendor Costs	All Other
Average Year 1 Cost	US$250,001 to US$500,000	US$250,001 to US$500,000	US$100,001 to US$250,000
Average Cost, Subsequent Years	—	—	—

Source: Vendor RFI

PATH FORWARD

Financial crime compliance is a heavily regulated area and one that is being transformed by technology. Understanding the solutions available from vendors is very important. Financial institutions and other regulated companies have choices in the market. The systems presented in this report allow for a firm to deploy on premise or opt for a cloud-first strategy; rely on vendor provided detection rules or maintain their own rules or AI models; among many other considerations. These vendors offer options that financial institutions need to support their financial crime compliance operations.

For Financial Institutions

There is no single best AML transaction monitoring system for all financial institutions. There are several good choices to meet almost any set of requirements. Every institution has its own unique requirements. This unique combination of factors, along with the organization's risk appetite, will influence the list of vendors meriting consideration.

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

We recommend that institutions looking for a new AML transaction monitoring system narrow their choices by focusing on four areas:

- **The art of the possible:** What can be done with advanced tools? Look at whether needed functionalities are available out of the box. Check to see what is actually in production.
- **The technology:** The overall architecture, the workflow and configuration tools and environment, and analytic capabilities may all be crucial considerations for a financial institution. Perform proof-of-concept exercises with shortlisted vendors. This is a chance for providers to show what they can do.
- **The vendor's stability, knowledge, and investment in the solution:** Consider the partnership dimension carefully. Key functional gaps are quickly closed by leading vendors—but be prepared for additional customization costs.
- **Implementation and support capabilities and experience:** Celent can help with selection projects; we know the vendors and the markets well.

For Vendors

As a group, AML transaction monitoring systems are expanding their capabilities rapidly through significant investments. The solutions are delivering a great deal of functionality with improved analytics and workflow, along with a widening spectrum of digital and AI/machine learning capabilities. Solutions are also more connected, with APIs and RESTful web services becoming the de facto standard. Although these trends are all excellent news for financial institutions, they 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.
- Continuing to build out configuration environments to put rules configuration, model development, and change controls in the hands of your clients. Configuration tools that business analysts can use get high scores from financial institutions assessing these solutions.
- Making implementation faster and less expensive.
- Continuing to expand functionality—especially in in the use of AI, analytics, and process automation capabilities.
- Investing in embedding cloud-first capabilities into the product.

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

APPENDIX: CELENT'S ABC METHODOLOGY

Celent actively reviews vendor systems in the risk management and compliance market. This report profiles 17 AML transaction monitoring systems and evaluates them according to Celent's ABC Vendor View and Transaction Capabilities Matrix.

To analyze the capabilities of AML transaction monitoring systems, we invited 40 software vendors worldwide to participate in Celent's research. Because some vendors chose not to participate or ultimately did not fulfill the participation requirements, the report features 14 fully profiled vendors and 12 fully participating in our ABC Vendor View analysis. The report also features three brief profiles on vendors that for various reasons did not participate in the RFI. There was no cost for vendors to participate.

Celent asked vendors to :

1. Complete a detailed RFI on Celent's VendorMatch platform.
2. Conduct a product briefing and solution demonstration.
3. Provide client references to take an online survey developed by Celent.

Each of these steps is described in the following sections.

VendorMatch RFI

Celent used its unique VendorMatch platform to gather RFI data from each vendor. VendorMatch is the world's largest vendor and solutions data store—combined with analytical tools—to help financial institutions find, evaluate, and select a solution. Each profile contains a link to the vendor's VendorMatch listing.

The RFI for this vendor evaluation study gathered responses on some 150 behavior detection, rules and analytics, case management, and reporting functionalities of AML transaction monitoring systems. The RFI also gathered information on eight other dimensions common to any system including company/ product information, technology base and scalability, deployment options, implementation, security and availability, commercial terms, and client base, as shown in the table below.

As part of the VendorMatch RFI process, Celent gathered much more information about each solution than is reflected in this report. Celent subscription clients can leverage advisory access to connect with the author and learn more about the vendors. Since the online database can be updated by vendors at any time, the online data may be more current than this report.

© CELENT

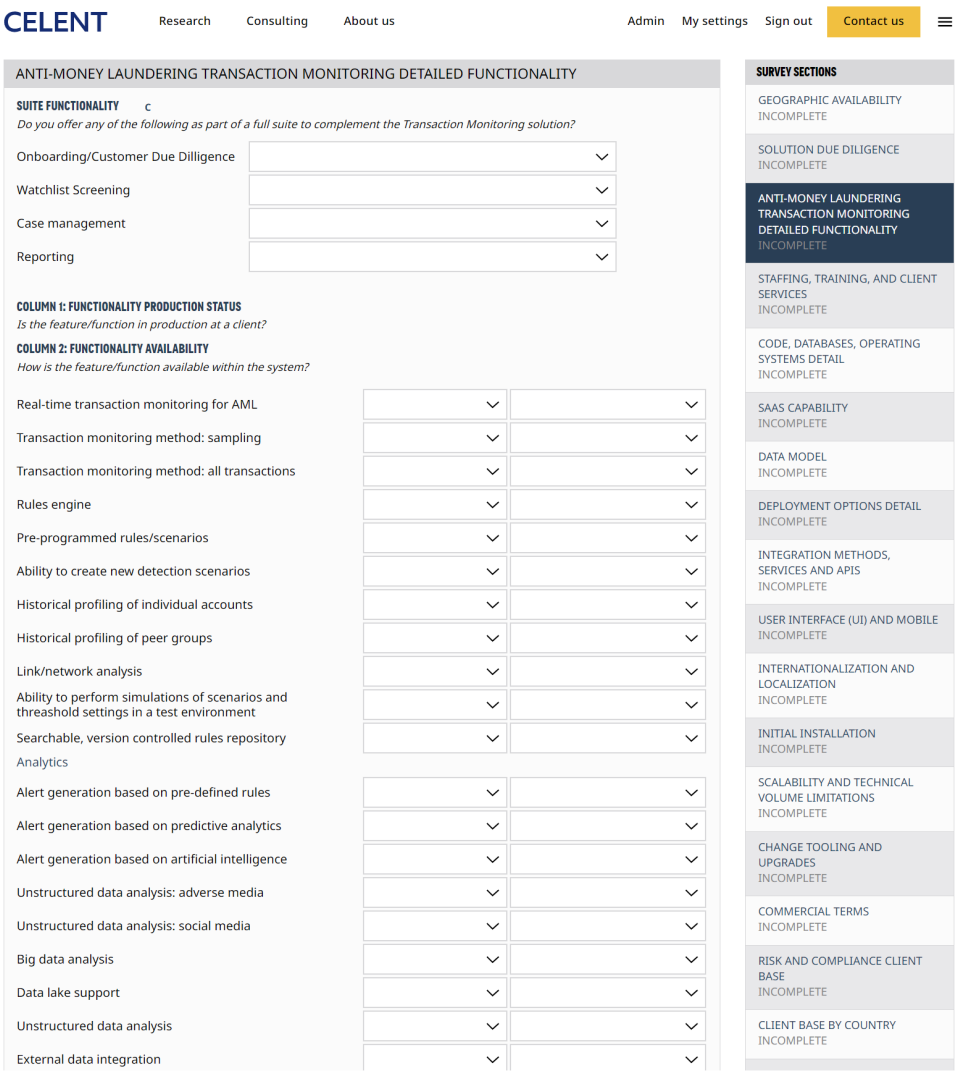
Table 18: Celent AML Transaction Monitoring Systems RFI

Dimension	Features
Company Information	Company overview
Product Information	Product overview, release history, and geographic availability
	Revenue from product
Functionality	AML Transaction Monitoring detailed functionality
	Support for currencies, languages, and local conventions
Technology	Code, databases, and operating systems
	Data model
	Scalability and technical volume limitations
	Integration methods, services, and APIs
Deployment	SaaS capabilities
	Deployment options: On-premise, hosted, private/public cloud
	Client base by deployment mode
Implementation	Initial installation, staffing, partnerships
	Change tooling and upgrades
Security and availability	Application security and cybersecurity
	Disaster recovery features
Commercial terms	Pricing models, factors, and average costs
	SLA service scope and features
Customer base	AML TM clients by financial vertical and tier size
	Clients by country
	Customer references

Source: Celent VendorMatch

The figure below illustrates one of the VendorMatch RFI data collection screens, the primary AML Transaction Monitoring functionality tab. Each solution type has a unique functionality tab, as well as functionality tabs common to all systems we review.

Figure 7: Celent VendorMatch RFI Data Collection (anonymized)



Source: Celent VendorMatch

Celent asked about availability and implementation status for each AML TM function, providing the vendors with the response options shown in the table below.

Table 19: RFI Functionality Response Options

Implementation Status	Feature Availability
At least one client in production (2)	Available out of the box (5)
Supported but no live clients in production (1)	Configurable using simple tools targeted for a business user (5)
Not supported (0)	Configurable using tools targeted for an IT user (4)
	Configurable through a scripting language/coding (3)
	Available with integration to a separate module provided by this vendor (2)
	Available with integration to a third party solution (2)
	Under development / On road map (1)
	Could develop—would be considered customization (1)
	Not available / Not applicable (0)

Source: Celent analysis
Weighting given to each response in parentheses.

Demonstration

Each vendor was provided the opportunity to present their transaction monitoring system to Celent analysts. Each followed a scripted agenda that focused on rules/analytics configuration, workflow, usability, functionality for internal users specific to AML operations, and the overall architecture of the system.

Customer Reference Feedback

Celent used an online survey tool to gather feedback from client references provided by each vendor. The survey asked about client views of the solution's business and technology value and assessed the vendor's customer service. The survey also asked each client what it liked best about the vendor and solution they use and solicited suggestions for improvement.

Customer reference feedback is presented in the Vendor Profiles, including a diagram that displays the average ratings given to the vendor in five categories. Each average rating includes up to 13 underlying ratings, as shown in the table below, scored by the customer on a scale of 1 to 5, where 1 means "very poor" and 5 is "excellent." It is advisable to keep in mind that the evaluations and comments may vary according to the specific needs of each reference client.

Table 20: Customer Feedback Survey Items: AML Transaction Monitoring Systems

Category	Ratings Included in the Average
Functionality *How would you rate the FEATURES you are currently using?*	False positives reduction Rules and analytics Historical profiling–Individual accounts Historical profiling–Peer groups Network/link analysis Other visualization tools Process automation Artificial intelligence Support for channels/products Currency and language support Audit trail
Technology *How would you rate the TECHNOLOGY of this AML TM solution in the following areas?*	Ease of system maintenance Flexibility of the data model Scalability of the solution Vendor's timing in improving technical performance through new releases and fixes Configurability of the solution Overall satisfaction with the technology
Integration *What has been your experience INTEGRATING this AML TM system with the following?*	Core processing systems KYC systems Watchlist screening and sanctions systems Third party transaction monitoring systems Third party analytics Internal applications and databases Internal data sources External data sources Reporting systems
Implementation *Thinking back to when you first IMPLEMENTED this AML TM 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 Knowledge of your business Knowledge of their solution and relevant technology Continuity with the implementation team—did the core team stay engaged through to implementation Overall project success
Support	Responsiveness (handling of issue resolution) Speed of issue resolution Project management (estimations, scope creep, etc.) Work completed on time

How would you rate this vendor's ongoing POST IMPLEMENTATION support in the following areas?	Work completed on budget Knowledge of your business Knowledge of their solution and relevant technology Communication—proactive communication of issues and changes Staff turnover Consistently meeting SLAs Roadmap delivery Customer feature requests heard and responded to Overall quality of professional services

Source: Celent

Criteria for ABC Inclusion

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

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

Limitations

Celent believes this study provides valuable insights into current offerings in AML transaction monitoring systems. However, readers are encouraged to consider these results in the following context.

Although we gathered comprehensive RFI responses, viewed system demonstrations for each solution, and conducted a customer reference survey, we could not confirm all the solution details and client base information self-reported by participating vendors. The initial data collection commenced in mid-2022, and the vendors have had the opportunity to update their profile information since that initial outreach.

Additionally:

- Celent's ABC methodology uses a normalized scale. In some cases, this can exaggerate quantitative differences, but its purpose is to make the graph easier to read.
- A vendor's suitability comes down to the needs of the institution compared to the insight offered by this analysis.
- The mix of vendors and platforms includes Celent subscribers and nonsubscribers. We make no distinction between how either is presented, nor does it affect our ratings.

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 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 and requirements. 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.

© CELENT

RELATED CELENT RESEARCH

Inflexion Point in Financial Crime Compliance
April 2023

Changing the Rules: The Evolution of Transaction Monitoring
February 2023

Digitizing the Risk Back Office: Five Themes for Risk in 2023
January 2023

IT and Operational Spending on Anti-Money Laundering: 2023 Edition
December 2022

Technology Trends Previsory: Risk, 2023 Edition
October 2022

Maximizing the Value of Adverse Media Monitoring: Enabling a Dynamic Risk Assessment Framework for Anti-Money Laundering Compliance
September 2022

Overcoming Transaction Screening Challenges with Advanced Technology
July 2022

Innovation in Risk: A Snapshot through the Lens of Model Risk Manager 2022
June 2022

Demystifying Cloud in Operational Risk Management: Growing Adoption, Expanding Horizons
March 2022

Improving Outcomes with Entity-Centric AML: Keeping A Razor-Sharp Focus on the Customer
March 2022

Transforming AML Investigation with AI: Righting the Automation Imbalance in Compliance Operations
January 2022

© CELENT

COPYRIGHT NOTICE

Copyright 2023 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
99 High Street, 32nd Floor
Boston, MA 02110-2320

+1.617.424.3200

USA
1166 Avenue of the Americas
New York, NY 10036

+1.212.345.8000

USA
Four Embarcadero Center
Suite 1100
San Francisco, CA 94111

+1.415.743.7800

Brazil
Rua Arquiteto Olavo Redig
de Campos, 105
Edifício EZ Tower – Torre B – 26º andar
04711-904 – São Paulo

+55 11 3878 2000

EMEA

Switzerland
Tessinerplatz 5
Zurich 8027

+41.44.5533.333

France
1 Rue Euler
Paris 75008

+33 1 45 02 30 00

Italy
Galleria San Babila 4B
Milan 20122

+39.02.305.771

United Kingdom
55 Baker Street
London W1U 8EW

+44.20.7333.8333

Asia-Pacific

Japan
Midtown Tower 16F
9-7-1, Akasaka
Minato-ku, Tokyo 107-6216

+81.3.6871.7008

Hong Kong
Unit 04, 9th Floor
Central Plaza
18 Harbour Road
Wanchai

+852 2301 7500

Singapore
138 Market Street
#07-01 CapitaGreen
Singapore 048946

+65 6510 9700