NICE Actimize

CELENT

White paper

Changing the Rules: The Evolution of Transaction Monitoring

Technology; Data and Domain Expertise in AML Suspicious Activity Detection

CELENT

CHANGING THE RULES: THE EVOLUTION OF TRANSACTION MONITORING

Technology, Data, and Domain Expertise in AML Suspicious Activity Detection

Neil Katkov

March 2023

This report was commissioned by NICE Actimize, which asked Celent to design and execute a Celent study on its behalf. The analysis and conclusions are Celent's alone, and NICE Actimize had no editorial control over report contents.

CONTENTS

© CELENT

EXECUTIVE SUMMARY

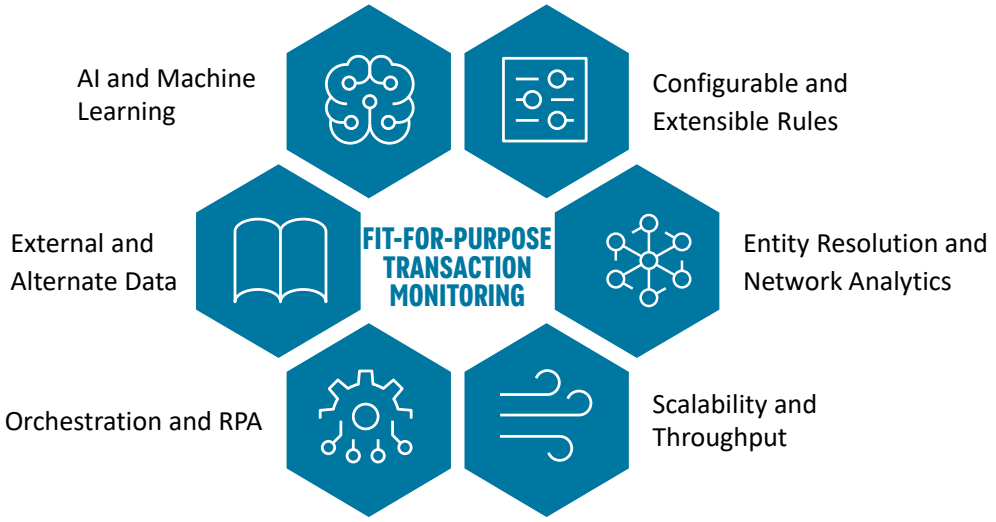
As financial institutions and regulated industries face ever more complex money laundering and criminal schemes, a sole reliance on rules is no longer sufficient. Advanced technology and modern techniques are moving the goalposts in the state of play for suspicious activity monitoring.

Anti–financial crime must keep up with the multiple and fast-moving risks of today's world. In addition to the many typologies by which criminals push illicit funds through the financial system, financial institutions are challenged to effectively counter the myriad of risks around:

- Black swan events such as COVID-19 and the conflict in Ukraine.
- ESG crimes like human slavery, environmental crime, and opioid trafficking.
- Other emerging risks.

Financial institutions need to move beyond check-the-box rules to advanced detection techniques that maximize the efficiency and effectiveness of anti–money laundering (AML) investigations. New approaches harnessing advanced technologies can help AML compliance operations optimize detection coverage based on business-specific risks and intelligently monitor entity-specific behaviors, while reducing false positives and manual work by compliance analysts.

Figure 1: Advanced Techniques Raising the Bar in Suspicious Activity Detection



Source: Celent

INTRODUCTION

Pressures emerging from the technology, business, and regulatory environment are creating new demands for financial crime compliance that existing processes are not always equipped to handle. New technologies and approaches are being deployed to cover gaps, increase performance, and enhance accuracy in AML behavior detection.

Regulatory Pressures

Regulators are increasingly focused on the ability of AML programs to accurately identify financial crime. The growing sophistication, depth, and breadth of money laundering schemes has led to specific legislation and guidance around beneficial ownership. This criminal activity has also led to increased regulatory scrutiny of shell companies and predicate money laundering offenses as well as guidance for pinpoint coverage for the constantly expanding universe of financial crime typologies. Fortunately, regulators are also beginning to embrace the potential of innovative technologies in dealing with these challenges and improving the efficacy of financial crime compliance.

Business Pressures

Digital and mainstream financial services alike are also seeking increased accuracy from their behavior detection technology to reduce the flow of exceptions that require manual analyst review and rein in the ballooning costs of conducting false positive investigations.

Technology Pressures

AML operations are being challenged to meet new scalability requirements and to develop more automated processes to support the pace of digital business. This applies to digital financial services at mainstream financial institutions as well as to payments, fintech, and other regulated online services such as gaming and crypto.

These pressures are exposing the well-known limitations of traditional AML technology and leading financial institutions of all sizes to leverage new technologies, analytics, and data sources. This new approach will help modernize the art and science of transaction monitoring.

© CELENT

CHALLENGES WITH THE TRANSACTION MONITORING STATUS QUO

Financial crime compliance in general and transaction monitoring in particular face a number of challenges. These include poor data quality, difficulty in covering complex and fast-changing typologies, and sky-high false positive rates.

Table 1: Challenges in Transaction Monitoring

	Challenges	Consequences
Internal Data	Issues with data gaps, data quality, and silos in internal data.	Affects accuracy and completeness of detection.
External Data	Inability to incorporate adverse media, to use UBO analysis in monitoring / risk assessment, or to enrich alerts with this data.	Missed risk signals from external data. Analysts need to manually assemble alert evidence.
Detection	Failure to monitor across channels, products, lines of business, and geographies.	Exposure to money laundering activity involving these multiple nodes.
Typologies	Focus on isolated indicators like cash velocity.	Inability to detect complex money laundering typologies.
Network Analysis	Rudimentary or nonexistent network/relationship analysis.	Inadequate insight into fund flows or entity relationships that might suggest suspicious activity.
Real Time	Lack of real time monitoring and real time transaction interdiction.	Exposure to money laundering risk in digital financial services, money mules, and other schemes.
Scalability	Inability to support industrial scale and throughput requirements.	Inadequate coverage of high-volume digital financial services, faster payments, etc.

Source: Celent

Data Quality and Availability

Data issues have been a hallmark of the AML technology journey since the beginning. Despite many improvements and a great deal of technology evolution, data remains a defining challenge for the industry. This is nowhere more evident than in transaction monitoring. Data issues confronting transaction monitoring range from poor, incomplete, and siloed internal data to difficulties in fully leveraging external

data. Moreover, the increasing use of AI and machine learning for AML is creating new data management challenges.

Limitations of Internal Data

Internal transaction and customer data are the fundamental inputs for transaction monitoring systems. Yet financial institutions often face data issues such as missing or incomplete data, inconsistent data, and duplicate records. Issues like these stem from data collection practices, multiple source systems and data models, and any number of line-of-business, operational, and technology factors. Incomplete or low quality data can affect the accuracy of behavior detection, impede entity resolution routines, and limit the ability of transaction monitoring and case management systems to generate network analyses to support investigations. Moreover, poor data can lead to gaps in monitoring coverage that could put the organization at risk from the compliance perspective.

In the early days of AML technology, getting source system data into transaction monitoring systems was an arduous process, often taking a year or more. Data management techniques at both banks and AML software vendors have advanced since then, and data feeds can now be set up in a matter of weeks or months. Yet issues with internal data quality persist and call out for new techniques to deal with them.

Aside from data quality issues, many institutions still use only a subset of their internal data, which limits their ability to detect suspicious activity. A frequent gap is failing to use nonfinancial transactions, such as customer address changes, in the behavior detection process, even though such transactions can signal heightened risk.

Some firms might not monitor transactions across all their delivery channels and transaction types. This may be due to limited support for channels and transactions by their vendor-supplied transaction monitoring system; because they have only implemented their system across a few channels; or because some products, such as trade finance or structured lending, are resistant to automated monitoring. Failure to monitor transactions across all channels, products, locations, or geographies, however, can expose a firm to financial crime activity that coordinates schemes across multiple nodes precisely to elude detection.

Difficulties Leveraging External Data

Another challenge in AML operations is making full, value-added use of external data. In the behavior detection context, external data is most often used to enrich the alerts sent to case management in order to provide additional intelligence for compliance analysts. Sanctions screening and adverse media screening results, information on external counterparties, and beneficial owner data are increasingly used to inform alert investigation. Analysis of this data is also crucial for identifying the links between customers and counterparties that may indicate more elaborate money laundering or criminal activity.

Traditional AML systems typically enrich alerts with sanctions screening results but are not set up to assemble the full set of data needed by analysts. In addition, external data such as adverse media may not be fresh, requiring analysts to—for example—resort to manual Google searches to look for the latest risk signals on alerted entities. These gaps in alert enrichment translate into additional time spent by analysts on manually gathering intelligence from various systems and sources to support alert investigation.

External data like adverse media and beneficial ownership analysis can also be used within the transaction monitoring process itself to resolve entities, enrich detection processes, support more accurate scoring and prioritization of alerts, and create in-depth network analyses of alerted activity, accounts, and counterparties. Status quo transaction monitoring processes typically do not leverage external data and so miss a valuable opportunity to strengthen activity monitoring.

Analytics and Detection Coverage

AML operations are engaged in a constant game of catching up with the demands stemming from evolution in digital financial services, the growing sophistication of money launderers and criminals, and the continuing onslaught of regulatory requirements. Traditional transaction monitoring analytics are challenged to keep up with these escalating requirements. Some of the coverage areas calling out for new technology and approaches include the following.

Trouble Keeping Up with Typologies

Traditional AML approaches typically lack suitable models and data to identify and monitor all financial crime threats, especially new and emerging typologies. Money launderers on the one hand and regulators, financial institutions, and AML technology on the other are involved in a continual game of whack-a-mole whereby tightening scrutiny of a financial sector, product, or geography results in criminals exploiting new sectors or devising new patterns for money laundering. Often, however, transaction monitoring rules rely on generic, isolated indicators such as cash volume/velocity or transaction thresholds. Even composite or nested rules may not be fit-for-purpose in detecting new and emerging money laundering typologies, which often involve networks of actors and transactions. Lack of appropriate data can also inhibit the detection of specific criminal activity such as human trafficking or smuggling of contraband.

A related issue is that many larger institutions run separate AML technology stacks according to line-of-business, operational, or geographic silos. This leads to fragmented detection analysis, making it difficult to detect money laundering typologies that involve multiple products, involve multiple locations, or cross geographical borders.

Limited Understanding of Activity Networks

It is increasingly vital to be able to identify connections between entities that signal likely money laundering, fraud or crime nexuses, money mule schemes, or simply exposure to high-risk entities. Many (but not all) transaction monitoring systems generate network or link analysis for use by compliance analysts. However, network analysis capabilities in traditional systems are often rudimentary. Network analysis outputs are sometimes presented in tabular, not graphic form, for example, and they require more analyst time to decipher. Traditional network analysis might only show which accounts transact with others. Network data of this sort that lacks enriched analysis such as frequency and monetary amount of transactions, or connections based on shared elements such as addresses, businesses, or beneficial owners cannot provide insight into the fund flows or entity relationships that might suggest suspicious activity. Similarly, network data that is unable to provide insights around external accounts will miss risk signals pertaining to their customers' counterparties.

At the same time, network analysis tools—whether rudimentary or state-of-the-art—can lead to overlong investigative exploration by analysts "digging" for suspicious activity and relationships. AML departments can respond to this challenge to analyst efficiency by developing policies to establish contours, such as number of hops, to network investigation. At the same time, some AML system vendors are starting to provide functionality aimed at improving network analysis efficiency. These tech enhancements include network visualization charts that are closely aligned to transaction monitoring alerts to more tightly focus analyst efforts. An emerging approach is to run AI and NLP-enabled models directly on network analysis results to automatically locate and generate pinpoint alerts on detected suspicious nodes.

Lagging the Digital Financial Ecosystem

Traditional AML transaction monitoring systems run their analyses in batch mode (even though fraud monitoring systems have for years provided real time capabilities). This works for many use cases, such as brick-and-mortar accounts or policies, as well as for forensic investigation purposes. However, digital financial services, fintech ecosystems, and faster payments are driving a need for real time analysis. Real time KYC assessments are already the norm for use cases such as digital account opening, quick loans, and alternative payments. Demand is now increasing for real time behavior detection in order to mitigate money laundering risk in digital financial services. Of concern here is the nexus between money laundering, fraud, and cybersecurity risk arising from digitization of financial services. For example, banks that can quickly identify and close down money mule accounts can thereby prevent the illicit transfer of these funds to offshore locations.

Taken together, such deficiencies in status quo transaction monitoring inevitably result in a limited ability to identify true positives that indicate real money laundering or other criminal activity.

False Positives

High false positive rates have been one of the most consequential issues facing AML operations because of their outsized impact on efficiency and cost. The wide net spread by dozens of rules often results in high false positive rates. Transaction monitoring systems have typically been plagued by false positive rates exceeding 90% of total alerts generated and often north of 95%. Put another way, for every 20 alerts investigated by analysts, 19 will prove to be false alarms. False positives from transaction monitoring and other AML systems directly fueled the rapid expansion of compliance analyst teams over the past decade, leading to soaring AML operations costs.

In recent years, machine learning has succeeded in reducing false positives by 50% to 70% or more. Despite this significant achievement, however, even banks that have implemented machine learning may have difficulty in controlling AML compliance costs, much less reducing them, as the continued expansion of regulatory requirements and the evolution of new financial crime typologies lead to increased complexity in AML technology and operations.

“ False positives from transaction monitoring and other AML systems directly fueled the rapid expansion of compliance analyst teams over the past decade, leading to soaring AML operations costs.

Impact on Investigation

Poor data quality, gaps in data availability, constraints in analytic and detection capabilities, and high false positive rates severely impact efficiency at the investigation stage. Despite their high volumes, false positives are the low-hanging fruit here and can now be resolved quickly. The limited ability of traditional systems to keep up with evolving typologies and the complex organizational strategies of criminals, however, leads to longer alert investigation cycles and generates an increasing need for large teams of highly trained analysts to adequately investigate alerts. More importantly, much of the data and analysis—such as risk scores or contextual adverse media results—needed for alert investigation isn’t automated through enrichment and orchestration. As a result, significant time and labor is lost to routine data collection work—such as searching Google and accessing various internal systems—instead of value-added investigation of complex suspicious entities and activities.

© CELENT

TRANSACTION MONITORING FIT-FOR-PURPOSE IN THE DIGITAL AGE

To be effective in today's world of multiple and fast-evolving risks, suspicious activity monitoring systems need to fire on all cylinders, leveraging rules, advanced analytical models, data, and domain expertise.

Detection Analytics

While artificial intelligence is enabling advances in anomaly detection, network analysis, and false positives reduction, it may be premature to declare the demise of rules. There are many reasons why rules are not going away anytime soon. Regulators continue to emphasize the use of rules to cover a wide variety of known risks. Financial institutions have also built significant domain expertise around rules. Firms also face challenges in developing and maintaining effective stand-alone AI models for financial crime detection. Issues such as these are leading many institutions to adopt a paradigm of leveraging rules and machine learning together in a hybrid approach. Meanwhile, incumbent AML vendors as well as regtech startups are offering systems that leverage both rules and machine learning for suspicious activity detection.

Table 2: Fit-for-Purpose Detection Analytics

Feature	Capability	Benefits
Curated Rules	Targeted, on-point rules library.	Detection for firm-specific risks while avoiding rules proliferation.
Configurability of Rules	Ability to create, modify, test rules and launch them in-flight.	Support baseline risks and response to new risks.
Coverage of Typologies	Rules and routines to capture typologies.	Effective coverage for existing and emerging typologies.

Source: Celent

Curated Rules

Detection rules have to a large extent been a tick-the-box exercise aimed at satisfying regulators that adequate controls are in place to provide a reasonable level of protection against obvious financial crime risks. This era is coming to an end as

regulators place greater emphasis on the effective identification of specific financial crimes. Financial institutions are under increasing pressure to provide coverage for specific, new, and emerging typologies as well as to increase their ability to identify this activity as it happens.

This emphasis on effective identification of true positives calls for a refresh of detection techniques by both financial institutions and providers of transaction monitoring systems. The emphasis should be on creating the right mix of rules to cover the risks pertaining to a firm's financial industry sector, customer base, and product characteristics. Rules libraries should be carefully curated to mitigate these specific risks—while avoiding a proliferation of rules that could lead to duplicate alerts and excessive false positives.

Configurability of Rules

Always an important feature of transaction monitoring systems, configurable rules become even more crucial with the increasing regulatory emphasis on identifying true positives. Technology elements that contribute to greater rules configurability include:

- Support for graphical rules creation by business users.
- Library of intuitively labeled rules elements/components to support streamlined rules creation and creation of complex rules.
- Built-in rules testing sandbox and capability to move rules into production instantly.
- Ability to change in-production models on the fly to maximize risk coverage or zero in on pinpointed typologies, entity types, etc.
- Ability to introduce new data fields into the rules model, including data fields for external data sources.
- Low-code/no-code platform to maximize accessibility and efficiency of use.

Coverage of Typologies

Detection engines need to augment traditional generic scenarios such as cash velocity with rules designed to identify money laundering and other criminal typologies. Numerous regulators such as FinCEN and organizations such as FATF document new typologies on a regular basis. At a minimum, detection engines need to have a library of rules and/or AI routines covering these recognized typologies; and regulators increasingly require this. Additionally, large financial institutions as well as industry consortia should work to identify risks in their specific organizations, industries, and markets.

Developing rules to detect these activities requires focused and evolving domain expertise, including in nonretail areas like correspondent banking, trade finance, and broker-dealing. Even large institutions with the resources to develop complex, targeted rules themselves will benefit from a vendor system with strong rules

coverage of typologies; for smaller FIs, the quality of built-in rules is a crucial requirement when selecting a transaction monitoring system.

Suspicious activity detection systems should also be capable of clearly labeling alerts with the specific typology that triggered an alert. The system should enrich the alert with the supporting evidence, such as transaction patterns and counterparties, and provide a natural language explanation of how the evidence constitutes activity indicative of the typology. Enriching, labeling, and packaging alerts in this way can automate much of the investigative process as well as support a more consistent and standardized approach to alert classification, review, and decisioning.

AI and Machine Learning

Perhaps the most proven use case for machine learning in financial crime compliance is false positives reduction. Machine learning that leverages both the previous decisions of human analysts and specific routines to identify obvious false positives can slash false positive rates by 50% to 70% or more. In addition to increasing efficiency in AML operations, this frees up compliance analysts to focus on value-added investigation of high-risk alerts. Machine learning aimed at reducing false positives is now becoming a table stakes feature of vendor-provided AML systems.

Table 3: Leveraging AI and Machine Learning in Behavior Detection

Feature	Capability	Benefits
Predictive Analytics	False positives reduction and suppression.	Increase compliance analyst efficiency.
Supervised Learning	Identify transaction sequences signaling financial crime risk.	Effective coverage for existing and emerging typologies.
Unsupervised Learning	Anomaly and pattern detection, cluster analysis.	Uncover unexpected or hidden activity. Correlate risks with customer segments.

Source: Celent

At the same time, we are seeing continuing advancements in the ability of AI models to identify true positive behavior. Much of this work is being done by internal data science teams designing models to run on AI platforms. Detection challenges that AI is making progress with include the following:

- Anomaly detection, the perennial challenge in AML suspicious activity detection of searching for the “unknown unknowns” that may signal suspicious activity. Anomaly detection using AI typically involves various unsupervised learning techniques.
- Identifying sequential or complex transaction patterns involving multiple accounts, products, or locations that may indicate the presence of money mules, abuse of financial products such as loans and insurance policies for money laundering, and criminal cells or organized crime rings. Trained or structured

learning approaches are prevalent here, including models used for detecting specific typologies.

- Qualifying and refining the results of traditional behavior detection by running the output from rules-based transaction monitoring systems through AI models.

> Machine learning that leverages both the previous decisions of human analysts and specific routines to identify obvious false positives can slash false positive rates by 50% to 70% or more.

Hybrid Approach to Rules and AI

Rules and AI/machine learning constitute distinct approaches to suspicious activity detection, and each has their own areas of strength. For example, rules benefit from decades of accumulated domain expertise and regulatory acceptance, while good AI detection models tend to have far lower false positive rates. Rules and AI also have specific operational requirements. For example, AI models require large amounts of data to train them, while significant time and effort typically must be spent to tune rules effectively. For these and other reasons, large financial institutions with sophisticated AML operations tend to use both rules and AI platforms for behavior detection, frequently running them in parallel, using AI models as a second-stage detection process following rules-based monitoring or using AI models for specific use cases.

Moreover, rules and AI models are increasingly being used together to optimize detection. Signals from rules can help to inform and improve machine learning models. Rules can also be combined with AI techniques to detect specific financial crime typologies, which are a particular focus of regulatory scrutiny. For such reasons, detection analytics can benefit from leveraging both fit-for-purpose rules and machine learning models to cover the wide variety of financial crime risks facing financial institutions and increase the efficiency of AML operations.

On the supplier side, AML system vendors are increasingly adding AI and machine learning capabilities to their transaction monitoring products. This makes it possible for even smaller institutions to leverage the advantage of advanced analytics in their AML operations.

© CELENT

Entity Resolution and Network Analysis

Obtaining a full view of customer risk is a fundamental concept in financial crime compliance, but achieving this holistic, 360-degree view has been an elusive goal for AML operations. New techniques are now enabling significantly enhanced insights into customers and potentially suspicious activity, patterns, and associations.

Table 4: Knowledge Graph Analytics Support Detection and Investigation

Feature	Capability	Benefits
Entity Resolution	Link disparate and siloed customer data, fill data gaps, and incorporate external data.	Support 360-degree, risk-aware monitoring and knowledge graph-based analysis.
Network Analysis	Expose linked accounts, activity, and personas, including external counterparties.	Automate and support alert and case investigation, and uncover hidden relationships/activity.
External Data	Incorporate geospatial, BO/director/controller, adverse media data into monitoring, network analysis, and investigation.	Enhanced risk insights into customers, associates/ counterparties, and owners.

Source: Celent

Entity resolution leverages rules, name matching, natural language understanding, and machine learning algorithms to connect disparate data on customers. A basic use case of entity resolution is to deduplicate customer or account data. Entity resolution is also used to consolidate multiple accounts associated with a single customer to create a complete customer persona for transaction analysis purposes (and also for KYC, screening, and forensic purposes). Because transaction source data is often not customer-centric but rather categorized by account or product, entity resolution enables more effective detection of activity stretching across multiple accounts, lines of business, or locations and involving multiple counterparty accounts and entities, including noncustomers external to the bank.

Network analysis is also being remade by entity resolution techniques. Traditional network analysis indicates links and transaction flows between accounts in graphical format. This is useful for spotting relationships between accounts but still requires compliance analysts to manually investigate customer and transaction details to search for indications of suspicious activity or criminal risk. Entity resolution-based network analysis performs much of this work for the analyst by assembling, consolidating, and analyzing available information on accounts and customers associated with an alert for presentation to the analyst.

External data can further strengthen the ability of entity-based network analysis to understand relationships and patterns between accounts. Geospatial data can be used to plot locations and distances of bank branches or customer and business addresses involved in transactions. Beneficial owner and director/controller data can be used to identify the nature and ownership of customers as well as external

counterparties. Adverse media screening can provide further insights into the potential risk of customers, associates, and counterparties. Performing entity resolution and link analysis on these potentially vast amounts of internal and external data requires modern graph databases and other Big Data analysis technologies.

Advanced network analysis is a powerful tool for alert and case investigation. Furthermore, by adding detection logic to automate the analysis of network information and generate alerts, network analysis can be used to perform transaction monitoring. This emerging approach should be particularly effective for identifying criminal rings involving multiple customers or businesses, including noncustomer counterparties external to the bank.

Shared Learning

Financial institutions have slowly been working toward data-sharing arrangements that can help improve risk detection on an industry-wide basis. A number of governments globally have been developing data-sharing schemes aimed at fighting financial crime. At the same time, open source as well as commercial technology providers are coming to market with federated learning software to support the secure and confidential sharing of data between financial institutions. A major focus is using federated data to improve models used in financial crime detection as well as to share financial crime typologies among the industry.

Cloud adoption is helping drive the sharing of financial crime intelligence. Some cloud-based transaction monitoring providers are leveraging cross-institutional data—with their clients' permission—to optimize machine learning models and make the improved models available across their client base. Such off-the-shelf models also make it possible for institutions to implement machine learning immediately, without requiring an extensive period to train models. This approach also enables smaller firms that lack internal data science capabilities to benefit from behavior detection supported by machine learning.

Scalability and Cloud to Support Digital Financial Services

Another challenge for traditional AML systems is scalability. The massive transaction volumes of large digital financial services and payments players demands high-performance systems capable of scaling to handle these volumes. Cloud-first AML systems that leverage containerization, APIs, and the high-performance computing and high-capacity data capabilities of cloud environments can help support both the throughput and connectivity requirements of modern digital financial services and ecosystems.

ORCHESTRATION TO SUPPORT ENHANCED COMPLIANCE

Financial crime compliance is moving to continual monitoring and assessment of risks in order to maximize accuracy and responsiveness to signals arising from changes in customer behavior and attributes. Orchestration of internal and external data streams to enhance transaction monitoring and post-processing data enrichment to drive efficiency in alert and case investigation are central enablers supporting this new paradigm.

Use cases for orchestration include:

- Supporting dynamic risk assessment throughout the AML value chain.
- Feeding internal and external data at the preprocessing stage to enrich monitoring data, ensure complete coverage of financial and nonfinancial transactions across the enterprise, and provide additional signals to support risk detection.
- Enrich postprocessing alert data to support more efficient analyst review at the alert and case investigation stage.

Dynamic Risk Assessment

Dynamic risk assessment involves integrating traditionally discrete stages of the AML value chain so that the analytical results of each process mutually inform and support ongoing analysis. This could involve using risk scores from KYC assessments in behavior detection models, and conversely adjusting the KYC risk scores according to insights derived from the detection system. Orchestration can also support the frequent adjustment of KYC risk profiles to reflect new risk signals picked up from continuous monitoring of watchlists and adverse media. This in turn would enhance the timeliness of the risk profiles passed to the behavior detection system and thereby improve the responsiveness of the detection process to new intelligence.

Data Enrichment

Data enrichment at the preprocessing and postprocessing phase can support enhanced monitoring and more efficient alert and case investigation.

© CELENT

Pre-alert data enrichment involves routines to resolve entities and to fill gaps in information, such as address, country, business, industry, or occupation. This helps improve understanding of customers, driving better segmentation and appropriate rules and analytics against each segment. Pre-alert data enrichment will also enrich understanding of networks, uncovering more and richer relationships in network analytics.

Post-alert data enrichment uses orchestration to create data pipelines that gather, assemble, and deliver targeted intelligence to support alert and case investigation by compliance analysts at the case management stage. This can include historical transactions, alerts, and cases; KYC profiles; beneficial owner information, percentages, and org charts; sanctions screening and adverse media results and scores for customers, beneficial owners, and associates; and pinpointed network and link analysis of the entities and other attributes relevant to the alert. Real time APIs play an important role in orchestration by making calls to gather specific data from internal systems as well as facilitating the delivery of third party external data such as beneficial owner data.

Alert and Case Investigation

Fit-for-purpose transaction monitoring should support efficiency, standardization, and effectiveness in alert and case investigation and regulatory reporting. Orchestration can automate the initial investigation work usually done by analysts and present curated “dossiers” ready for analyst review and additional investigation as needed at the case management stage. AI-supported orchestration and alert enrichment can help ensure that the data and assessments that go into an alert file have gone through an objective process to support more standardized review and decisioning. Finally, natural language generation, another branch of AI, can autopen and populate alert decisions and SAR case narratives for review, amendment, approval, and filing with regulators.

TOWARD A MORE EFFECTIVE COMPLIANCE PARADIGM

The technologies and techniques explored in this report represent a significant evolution in supporting an effective end-to-end approach to anti–money laundering compliance.

Putting the pieces together, elements that are remaking and enhancing the AML value chain include the following.

Data

- **Data prep.** Prepare data for processing by the detection engine: consolidate siloed data, deduplicate, fill data gaps, cleanse and standardize data.
- **Comprehensive internal data.** Leverage transaction data and customer data, as well as data across multiple channels, products, and locations (as fits the use case) to detect complex risks.
- **Incorporate external data.** Use structured and unstructured external data to enhance detection, enrich network analysis, and support investigations.

Detection

- **Rules.** Configurable and extensible rules tailored to the institution's risk. Agile rules configuration and testing. Coverage of money laundering typologies.
- **AI/machine learning.** Detection of anomalies, sequential/complex activity, and new typologies. Explainability of detected activity. Segment/rules optimization. False positives reduction.
- **Hybrid use of rules and AI.** Signals from rules to improve AI models. Rules/AI combined to detect money laundering typologies.
- **Shared learning.** Data-sharing and federated learning to improve detection models and to share typologies.

Enrichment and Analysis

- **Entity resolution.** Unite disparate customer/account data for effective detection of complex activity.

- **Network analysis.** Entity resolution and external data to understand risk in account relationships, beneficial owners, and counterparties. Detection logic to alert on high-risk nodes for focused investigation.
- **Orchestration.** Support dynamic risk assessment across AML processes. Coordinate internal and external data feeds to prep/enrich data for processing. Enrich alerts with UBO, network, etc., results to support analyst investigation.

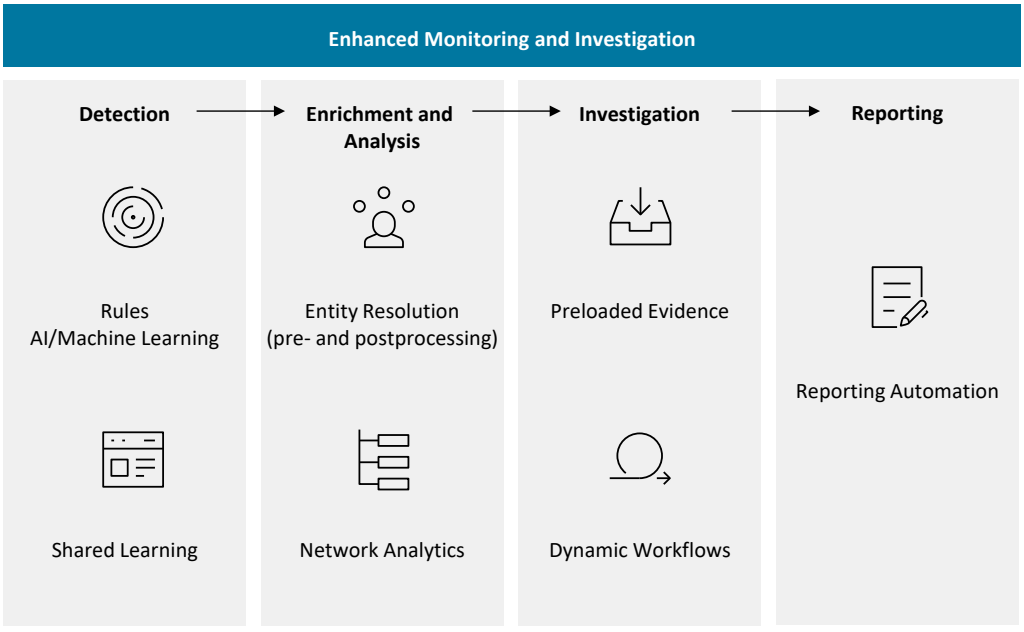
Investigation

- **Alert and case investigation.** Serve up enriched, curated "dossiers" to analysts for investigation to support efficiency and objectivity. Automate case and reporting processes.

Support for Digital Financial Services

- **Real time** monitoring/interdiction and **industrial scale/throughput** to enable effective monitoring for high-volume environments.

Figure 2: Technologies and Techniques Supporting the Enhanced AML Value Chain



Source: Celent

Many of the techniques and technologies supporting the enhanced AML value chain can be leveraged at multiple stages and for multiple use cases. Entity resolution is a good example. The name-matching, data linkage, and data wrangling techniques behind entity resolution can be used at the preprocessing stage to prepare and enrich internal customer and transaction data for behavior detection analysis.

Postprocessing, entity resolution can support alert enrichment and construction of knowledge graph-based network analytics to support investigation and review. As financial institutions and technology providers alike work with new technologies to support AML processes, we will see continued evolution in the way these technologies are used to drive advances in transaction monitoring and across the AML value chain.

© CELENT

PATH FORWARD

What does the future of transaction monitoring look like?

Despite the potential of harnessing advanced technologies to enable end-to-end automation of 100% of the AML value chain, financial institutions—and regulators—are unlikely to take that leap for some time. No matter how automated the front office and customer-facing functions—including KYC at onboarding—become in digital financial services, the core financial crime compliance process of transaction monitoring (as well as exceptions from KYC processes) still rely on compliance analysts reviewing alerts in the back office. At least in the midterm, the need for "bank-ready" transaction monitoring and case management systems is not going away—and at fintechs and newly regulated sectors, the demand for robust core AML systems is increasing.

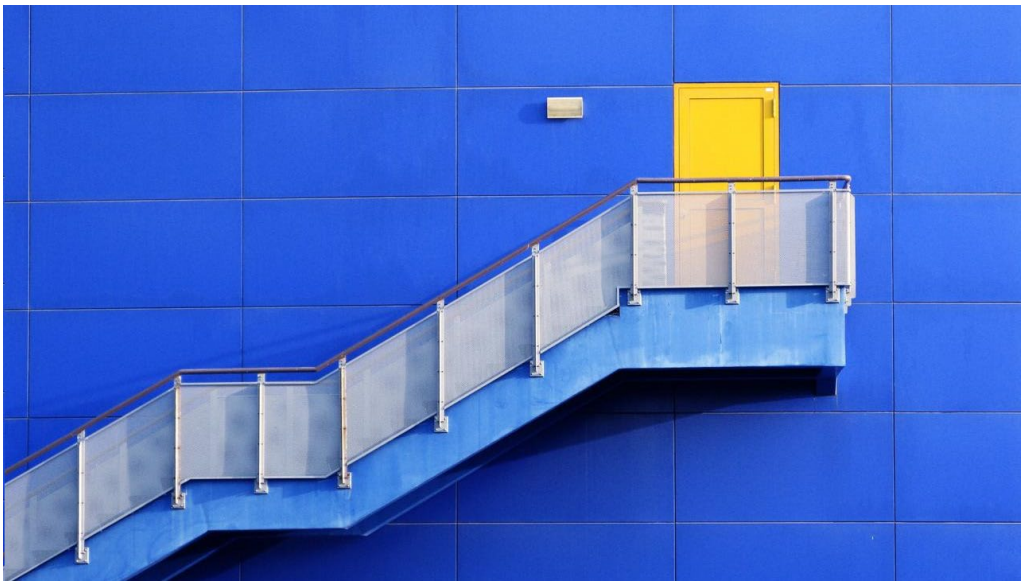
Advanced technologies like AI, Big Data analysis, and high-performance computing and new techniques such as API-enabled orchestration and data enrichment are making a difference in supporting increased accuracy and coverage of detection, automation of workflows, and support for enhanced and more efficient investigation at the case management stage.

Recommendations for Financial Institutions

Financial institutions should assess where and how these new technologies can benefit their financial crime compliance program. A common thread among fit-for-purpose transaction monitoring techniques is AI/machine learning, which supports optimization of customer segments and rules, preparation of preprocessing data, robust entity resolution and network analysis, alert enrichment, orchestration, false positives reduction, and automation in alert and case investigation and reporting.

- **Large financial institutions** with in-house data science capabilities will need monitoring systems that support the creation of analytic models and/or can ingest models created by their data scientists or third party models.
  - Large institutions have a choice between building/assembling data enrichment, orchestration, and investigation automation capabilities themselves, or to opt for an off-the-shelf solution to support modern transaction monitoring and case management.
- **Midtier financial institutions** that lack internal data science capabilities should consider moving to modern systems that offer prebuilt detection models as well as orchestration, alert enrichment, and investigation automation capabilities.

All financial institutions will benefit from a vendor with domain expertise that can support the development and use of rules and/or AI routines to detect money laundering typologies as well as unknown and emerging risks.



© CELENT

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

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