



Key Challenges in AML Transaction Monitoring Implementations

Whitepaper by

Sameer Pendse

Vice President, GRC - Industry Solutions Group

Amin Charania

Associate Vice President - Financial Crimes Solutions



***Anti-Money Laundering
(AML) Transaction
Monitoring [TM]
implementations are
ubiquitous across all tiers
of institutions as the level
of complexity of financial
crimes is on the rise***

Introduction

Anti-Money Laundering (AML) Transaction Monitoring [TM] implementations are ubiquitous across all tiers of institutions as the level of complexity of financial crimes is on the rise. The level of sophistication of the TM platform varies as we move across tiers. This paper discusses some of the challenges faced by Financial Institutions (FIs) in implementing TM platforms. Though the challenges could apply to all sizes and nature of FIs, the scope of this paper is specifically for challenges at top-tier and mid-tier financial institutions.

The challenges faced by the FIs can be organized into the following 5 categories:

- Span of the FI – the geographical, entity & LOB and instances/expanse of applications can pose specific challenges
- Data availability and quality is a key issue most FIs grapple with
- Configuration of business rules and the TM platform has a significant impact on how well the TM implementation works
- Infrastructure selection and maintenance choices decide how effectively the TM platform performs
- Cognitive computing is emerging as the new imperative with smart data, rule based computing and machine learning techniques being used increasingly for eliminating false positives and for detecting more complex alerts

Subsequent sections of this paper discuss each of these categories in more detail.



The span of the FI

The span of the FI creates implementation complexity in terms of the databases, applications, LOBs, countries/entities to be modeled in the target solution. In FIs where AML has been implemented for several years, it is more than likely that the architecture includes multiple types of AML TM platforms (e.g. Actimize, Oracle, other older products) at different versions, sometimes even from the same vendor. These TM platforms, for each LOB, can be at the regional cluster level or even at the country level in a single data center or across multiple data centers. With constraints of data secrecy acts, FI internal LOB level policies and volume of business in the region, decisions have to be made about whether to have a single TM target platform or cluster based instances.

In addition to the diverse and disparate TM platforms, there can also be a plethora of transaction processing platforms due to the span of the FI. It is not unheard-of to find multiple core banking platforms, multiple trading platforms (by product being traded) and multiple asset management platforms. Even if we do not consider having a holistic AML solution across an FI (a dream state), there is significant complexity involved in bringing transaction and product data into the target TM platform and mapping the source data structures to the target data structures for upload. While the core systems are covered fully during implementation, the business world is dynamic where addition of new sources, products during the lifespan of an AML platform is not uncommon.

One such instance is where a bank wanted to expand its business in Qatar in view of its bid to host Olympics. It had major challenges in adding the new instance on the existing platform due to its capacity, lineage and configurations. While these issues could be reconciled with time, it was a block for the bank to get compliance clearance for its business.

The challenges for each bank is unique. And so should be the implementation of AML systems

Our experience over the years in implementation of AML systems have enabled us to foresee and provide valuable consultation to our clients for a future proof implementation. This will get them closer to holistic transaction monitoring with a singular view of the AML risk posed by the FIs customers across LOBs.

Data availability & data quality

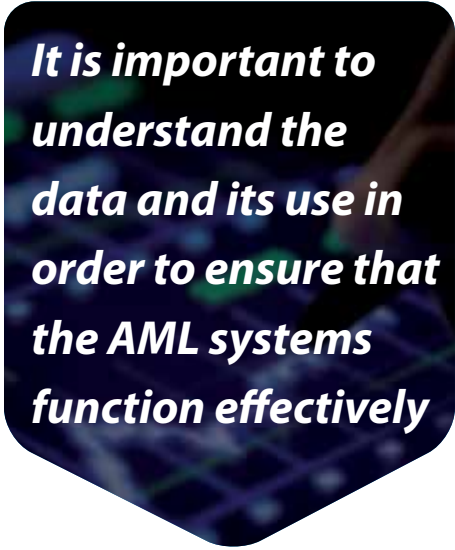
For a long time, the focus of IT was on the elegance and quality of computational logic. Data is once again, being recognized over the last couple of years as the driver behind effective computing results. The smartest platform in the world can be quite ineffective without high quality (integrity, consistency and completeness) data. The same principle applies to TM platforms. TM systems are one of the biggest consumers of data generated across the Financial Institutions. Huge investments have been made by FIs to create a 'golden set' of data for AML and other consuming banking systems. In spite of the rigor on data quality, the vision is far from being achieved due to limitations in the way the data is consolidated, aggregated and made ready for consumption. In our view, this attempt to create a golden set has, to some extent, added to the problem as there could be more than one golden set now within the bank.

Assuming we are able to overcome the challenges and are able to create a golden repository within the FI, the systems today still have limitation in deducing meaning of the data.

Even with the advancement of AML platforms available today, the information hidden within the data presented along with the AML alert still has to be analyzed manually. AML systems typically need derived data (like pass through flag, cross border flag, correspondent bank relationship, summaries and profiles) from the base data set. As the base data set is received from diverse systems, if the derivation logic is unable to consistently ascertain the data across systems and different transactions, the detection logic in the TM platform with attendant thresholds and rules may or may not be effective. This can lead to a large amount of false positives and worse, missed alerts.

A straight forward solution to this problem is to recognize that actually implementing a TM platform consumes a large amount of surround effort such as data engineering and configuration definition (see next section), and there is a need to budget and plan this effort. A more sophisticated approach would use 4GT tools for data analysis combined with statistical sampling as well as creating specialized data validation

and enrichment scripts to tackle this problem (while having data engineers in attendance with business representatives in solving this problem).



It is important to understand the data and its use in order to ensure that the AML systems function effectively

Another important consideration in the presence of a large number of data sources is the need to ensure that the data sources are prepared and loaded into the TM platform in the right sequence to address inter-dependencies. It would make no sense for the data to be patched together in the wrong sequence or with the wrong attributes; it will completely defeat the purpose of having an AML automation platform. The right data designers can help solve this problem.

It is a compliance and business nightmare to realize there is an exception in data ETL process, where a type of data set or attribute is not translated as required because it could not be covered by the logic implemented. The systems today have limitations in catching any exception due to a change in upstream systems that may not necessarily be done in consultation with the AML system. Such situations are not as uncommon as one may think them to be. The recovery and mitigation of risk after such discoveries are painful.

Moving to a smart data representation where all the data is brought together in a semantic graph can reduce such instances, while reducing the cost and efforts of continuous enhancement to ETL in order to meet the dynamic business changes.


Configuration

The output of an AML system is only as good as it is configured to be. Most AML systems today implement a risk based approach through implementation of multifarious rules, thresholds and scoring. The configurations of these rules and the perception of risk differ with each FI, which highly impacts their implementation. The product which works well for a particular FI may not provide the same experience to another if the configurations do not rightly reflect the organization wide risk models and perception. Having said about the business heavy configurations, there can be some technical configuration which can cause pain by overriding the business requirement with its technical implementation. A particular technical configuration, which would run a process to consolidate/validate flags being switched off for improving 'performance' is not unheard of. The flags would still be available and system would still work, however it may mean more attention and focus from business users in analyzing the alert. This may typically happen when the system capacity to process increasing volumes throw a challenge to choose quality over adherence to a minimum set of AML requirements

Apart from the system level configurations, periodic configuration changes to TM platforms are critical too. While implementing a new system these configurations can be done as an iterative exercise with 'n' cycles (typically 3-5 cycles) for tuning of scoring, thresholds and policy rules to ensure that no alerts are missed and false positives are also capped. If it is a migration from an existing legacy system, there can be a parallel run between extant systems and the target TM platforms over a period of 2-3 months, once the summaries and profiles are built on a new system (typically with 6 months of historical data). This approach is effective in validating the closeness and deviations between the two set of systems and ensuring that no new risks are inherited or at the least mitigated with the implementation of new AML system.

Business and compliance have a large role in the business configuration phase as they need to participate in the analysis of alerts and subsequent tuning efforts.

Apart from the business configuration, there is also a burning need to ensure that the TM platform (including the case manager) aggregates and consolidates related alerts so as to ensure that the right exposure is being investigated holistically. It is also important to configure the alert investigation workflow and entitlements to ensure that the FIs processes are followed as well as to ensure that access to alerts for specific customers is controlled.



The advent of semantic technology can take away a lot of efforts and time required to maintain such critical and voluminous configurations

While most FI now use statistical models to address the problem of implementing the right value for a rule parameter, it is still a complex and reactive approach as any change is the pattern of business data needs to be analyzed afresh (mostly post-facto). The false positive generation in this period is typically addressed by redirecting resources for handling these 'peak' periods. The change in configurations cannot be implemented instantly without a thorough assessment and testing.

The advent of semantic technology can take away a lot of efforts and time required to maintain such critical and voluminous configurations.



Infrastructure

Today most of the AML TM systems generally provide alerts for transactions on 'T + 1', where T is the day on which the transaction is posted in FI core systems. The AML system generally executes a 'batch' to generate alerts. The time required to complete the batch is directly proportional to the volume and capacity of the server. The estimations and forecast done while implementing the AML platform are highly critical however we must factor in the unforeseen business dynamics over the lifespan of the AML implementation.

When the batch processing time for an instance is high, any issues in the EOD processing with the upstream system directly impacts the time and efforts required for recovery of the AML batch to make it up-to-date. Even though, the recovery SLA associated with AML TM system are typically less stringent than other real time/core systems in the FI, it is critical that the TM platform be correctly sized for targeted performance in view of increasing anticipated business volumes and the approach taken for setting up instances at country/hub level. We have been involved in resolving a challenge to recover ~ 3months of processing to incorporate an

addition on source system in the last quarter. Each batch typically required 14-16 hours for 1 day of processing to be completed. By implementing tuning and automation (process and technical) for high efficiency batch processing and with some exceptions approved by business, the recovery was completed within 20 odd days. We believe such scenarios (in varying degree) would be observed by most FI who have implemented an AML system.

Sometimes it is not the upstream system but the technical patches on infrastructure products such as the database, the network and the ancillary applications that get the AML system out of service. Ensuring that the infra changes (big and small) are assessed and applied in the right order is of utmost importance. Obscure TM platform failure can result in hard to detect issues, if this assessment of infrastructure changes is not done with required rigor. These failures can hold up processing for days in a worst case and lead to regulatory non-compliance.

Cognitive Computing

Cognitive computing is the new wave and there are a variety of ways in which cognitive computing and smart data platforms can be used for complementing the efforts of TM platform implementation. Some of these are articulated below. While their theoretical value is undeniable, these are yet to be proven in the field on a large scale and the challenge to their adoption is one of mind-set, intent and regulatory approval rather than technology:

- **Smart data aggregation** – When the number of source systems/applications and databased cross the number of 20, it makes sense to aggregate all the data from the disparate systems into a smart/graph database. Subsequent extraction of consolidated data from such systems for loading into the TM platform then becomes easier. It also facilitates the elimination of the swivel chair effect (see point 2).
- **Investigation of false positives** – while rule based and machine learning systems may not reach the holy grail of auto-suppression of false positives due to regulatory implications, the ability for these systems to store smart data and facilitate investigations by eliminating the swivel chair is key. These smart data and graph based databases ensure that annotated data is available to the investigator automatically; once loaded it eliminates the need to reach out into separate systems to do the analysis. The cognitive solutions can also learn investigation patterns for specific alerts and ensure that subsequent investigations follow the same pattern as learned before, hence speeding up the investigation effort.
- **Investigation rigor** – Rule based and learning cognitive solutions can detect alerts which have been hitherto difficult to detect. An example is the Mphasis NextAngles smart compliance solution that can detect certain trade finance based alerts, which have so far been complex to detect e.g. over or under invoicing.



What Mphasis can do for you

Mphasis provides services (consulting, technology & process outsourcing) around AML TM implementations:

- Implement and tune smart compliance solution (NextAngles) for false positive investigations and identify alerts for trade finance based AML
- Define or re-engineer business configuration (scoring, thresholds, policy rules)
- Write business requirements, functional requirements and build POCs
- Evaluate vendors (for traditional supplier lifecycle management)
- Implement or upgrade a vendor platform like Actimize SAM, eRCM and Oracle Mantas
- Data engineering – data quality management (completeness, integrity, purity)
- Provide skills for AML alert triaging



Sameer Pendse

Vice President, GRC - Industry Solutions Group

Sameer has over 24 years industry experience in banking domain across the UK, USA, Far East and India. He has helped banking and capital market prospects & customers to build transformation programs using products and services. Some of the solutions he has provided include next generation banking, full banking service stacks and re-engineering risk management products. He has led various consulting engagements - Banking Transformation @ SocGen Romania and others. Sameer is a B.E graduate, specialized in AI & Parallel Processing and a GARP FRM certified.



Amin Charania

Associate Vice President - Financial Crimes Solutions

Amin Charania has 16 years of industry experience across the US, Europe and Asia. With his extensive business knowledge, Amin has delivered, led and consulted various banking and FinCrime implementation programs for some of the marketing leading products. He has managed compliance and legal portfolio for several years to provide strict vigilance of system operations, deliver business needs and mitigate BAU challenges. He is currently leading research and development of innovative frameworks and accelerators.

About Mphasis

Mphasis is a global technology services and solutions company specializing in the areas of Digital, Governance, Risk & Compliance. Our solution focus and superior human capital propels our partnership with large enterprise customers in their digital transformation journeys. We partner with global financial institutions in the execution of their risk and compliance strategies. We focus on next generation technologies for differentiated solutions delivering optimized operations for clients.

For more information, contact: marketinginfo@mphasis.com

USA

460 Park Avenue South
Suite #1101
New York, NY 10016, USA
Tel.: +1 212 686 6655

UK

88 Wood Street
London EC2V 7RS, UK
Tel.: +44 20 8528 1000

INDIA

Bagmane World Technology Center
Marathahalli Ring Road
Doddanakundhi Village, Mahadevapura
Bangalore 560 048, India
Tel.: +91 80 3352 5000



www.mphasis.com