The Importance of a Strong AML Transaction Monitoring Governance Framework in Today’s Regulatory Environment

Issue

Expectations for transaction monitoring (TM) governance are quickly evolving due to the complexity of detection systems, the demand for additional operational oversight, increased regulatory scrutiny, and the need for an adequate control framework to guarantee proper risk management. As a result, compliance officers/AML officers/money laundering reporting officers (collectively, MLROs), along with other affected financial institution personnel, are finding it increasingly difficult to manage their existing responsibilities amid the heightened scrutiny and expectations regulators have regarding transaction monitoring systems and the end-to-end (E2E) processes tied to them (e.g., vendor selection, tuning rationale, model validation requirements, backlogs, etc.).

Challenges and Opportunities

In our experience, organizations face multiple challenges with respect to designing a strong TM governance control framework. These include:

- **Managing regulatory expectations** – In addition to overseeing the day-to-day operations of clearing alerts and performing investigations, regulators expect institutions nowadays to ensure the integrity of the data, tune/enhance monitoring scenarios, and validate the effectiveness of the systems on an ongoing basis.

- **Tuning methodology and know-how** – Some institutions may lack the expertise in this area to develop scenarios effectively, fine-tune them, and ensure they are designed to cover known money laundering red flags. In some cases, this may be due to the fact that institutions relied on vendors/consultants to implement the TM systems, and never retained the knowledge within the organization. When presented with questions by auditors/regulators, MLROs may be unable to respond with the level of knowledge or detail that is expected.

- **Liaising with multiple parties** – TM programs depend on critical inputs provided by the business team about how products are intended to be used by customers, as well as on inputs from the compliance team about money laundering red flags/typologies associated with each product. Lack of collaboration between compliance, business and technology teams inhibits an informed scenario-tuning process that is based on data and the expert judgment of end users and risks.

- **Achieving global consistency** – For larger institutions with a global footprint, ensuring each region has hired the right people, implemented adequate detection scenarios and instituted strong controls to manage the end-to-end TM process has become a significant challenge. This is due to geographical distance from the head office, differences in regulatory requirements, and misinterpretation of regulations and/or internal policies and procedures.

- **Managing the alert investigation team** – The teams involved in the alert review process may be growing quickly, making it difficult to ensure that everyone on the team has the required skill set
and expertise to review the output of the TM systems (alerts). It also may be difficult within a rapidly growing unit to manage the quality of the rationale used by investigators to close an alert or to escalate it and document suspicion. Some larger institutions may offshore the alert review process, which adds to the difficulties in providing oversight, guidance and timely feedback.

- **Measuring success/effectiveness** – Traditional numbers-based metrics do not show the full picture when it comes to TM efforts. Many institutions struggle with determining how best to measure success since efficiency benchmarks alone do not guarantee effectiveness.

A strong TM governance control framework enables the institution to overcome the above challenges and presents various opportunities, such as:

- **TM E2E operating model** – Designing an end-to-end operating model provides financial institutions the opportunity to create a roadmap for how they want the TM process to function, including policy and procedure design, system selection, scenario calibration/tuning, alert review, suspicious activity report (SAR) filing and management information reporting. The model will also help in designing the control framework and an ongoing review process to ensure there are continuous enhancements to the overall process.

- **Creating a separate TM unit** – Designating a TM officer and allowing a separate unit to manage the end-to-end transaction monitoring process will allow the financial institution to understand clearly and manage all risks associated with this process, as well as have clear accountability of the function. A separate TM unit will also be better able to retain the proper skills needed to manage the people, process and technology side of transaction monitoring. In addition, a separate unit will allow for clearer lines of communication among different areas of the financial institution (i.e., IT, business and compliance).

- **Applying global minimum standards** – When looking to achieve global consistency, developing minimum TM standards that take regulatory requirements and industry-leading practices into consideration and adopting them throughout the different regions will ensure the group is operating at a known base level and managing money laundering risk consistently and effectively.

- **Measuring success** – Having a strong TM program that takes risk management into consideration allows institutions to present to senior management actual success factors and not just escalated cases and SARs filed. Success should be represented by a combination of the alert-to-SAR ratio and the following factors:
  
  - Being able to articulate clearly which known money laundering risks (red flags) are mitigated by the scenarios that were implemented;
  - Generating effective scenarios that highlight unusual activity, to assist in preemptively identifying activity that may later be flagged and referred by law enforcement;
  - Documenting a robust tuning methodology (inclusive of change control documentation and rationale for tuning) that is acceptable to regulators; and
  - Having adequate policies and procedures and experienced personnel to investigate the alerts generated by the TM system.

**Our Point of View**

In order for financial institutions to meet current regulatory expectations, they should develop a strong TM program – one that has a proper governance framework and oversight with effective, sustainable and repeatable processes and controls. This can be achieved by implementing a comprehensive operating model that covers the E2E process (i.e., system selection, scenario selection, tuning, alert review, SAR filing, management information reporting, and continuous review/validation and enhancement) to ensure adequate money laundering risk management.

Based on our experience, it is often useful for MLROs to assess the time and effort required to lead a strong TM program and determine whether the organization would benefit from creating a separate function to manage these responsibilities. Normally, larger financial institutions are more inclined to do
this; however, some smaller institutions may also see benefits in having a separate unit and officer responsible for the process.

Successfully managing the TM program also consists of understanding risk. Some products or business lines may pose minimal risk – for example, those with low volumes and values of transactions, those with strong controls around transaction limits, or those where customers cannot easily initiate transfers. A proper risk assessment should be performed to determine which products, services or regions pose the highest risk and do, in fact, require automated monitoring and more attention.

Lastly, to achieve global consistency, larger institutions with a global footprint should design and implement a set of minimum TM standards that should be adopted by each region. The regional units should only deviate from the adopted minimum standards in order to increase their controls to meet more stringent local requirements.

Institutions should consider the following points when developing minimum standards:

- Vendor selection (minimum automated system requirements)
- Product, transaction and customer coverage based on red flags
- Data inclusions/exclusions
- Minimum risk-based scenario set (taking CDD information into consideration), scenario selection, tuning processes and documentation
- Training standards customized for each role in the end-to-end process
- Investigation standards, including maintenance of supporting documentation and timeframes for completing reviews and filing SARs
- Metrics for generating management information reports that can be used to measure performance and risk, and identify enhancement opportunities
- Ongoing validation of the TM system (including recalibration of scenarios based on lessons learned from SARs filed) and the end-to-end process

How We Help Companies Succeed

Our Risk and Compliance professionals focusing on AML technology, teaming up with our model risk experts who include Ph.D.-level professionals with deep quantitative skills, can help your institution articulate and maintain a sound and robust AML transaction monitoring function. We have experience with a number of AML transaction monitoring systems on various platforms including, but not limited to, Actimize, Detica NetReveal AML (Norkom), Mantas, SAS AML, and FISERV, as well as a number of other systems. Our clients include banking and non-banking financial institutions of varying size and footprint.

Our AML transaction monitoring technology services include:

- Developing transaction monitoring target operating models and control frameworks
- Evaluating and selecting AML transaction monitoring systems
- Implementing and managing AML system implementations
- Developing and executing a sound and efficient scenario tuning methodology and approach
• Performing any or all of the following tasks by acting as an independent team:
  o AML red flag gap analysis/worst-case scenario analysis
  o Data validation
  o Scenario logic validation
  o Threshold values validation
  o Customer segmentation validation
• Recommending improvements to scenarios/thresholds

**Example**

A large global bank sought our assistance to enhance its current AML transaction monitoring systems and functions. This involved assessing the current organizational structure and control framework, designing a target operating model, developing policies and procedures, and evaluating and enhancing detection scenarios.

Together with our client, we developed a strategy and implemented a methodology for performing initial and continuous assessment of the institution’s risk. Specifically, we identified source systems and transaction codes, ensured accurate data feeds, selected scenarios aligned to the institution’s risks, performed quantitative analysis to calibrate the systems, used the analyses and available KYC data to segment the customer base in a meaningful manner, and tested the output and effectiveness of the generated alerts to drive further recalibration of the thresholds and scenarios. Furthermore, we deployed the target operating model we had developed with the client to ensure the entire group was managing its money laundering risk in a consistent and effective manner.

**About Protiviti**

Protiviti ([www.protiviti.com](http://www.protiviti.com)) is a global consulting firm that helps companies solve problems in finance, technology, operations, governance, risk and internal audit. Through our network of more than 70 offices in over 20 countries, we have served more than 35 percent of FORTUNE 100® and FORTUNE Global 500® companies. We also work with smaller, growing companies, including those looking to go public, as well as with government agencies.

Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

**Contacts**

<table>
<thead>
<tr>
<th>Carol Beaumier</th>
<th>Bernadine Reese</th>
<th>Carl Hatfield</th>
</tr>
</thead>
<tbody>
<tr>
<td>+1.212.603.8337</td>
<td>+44.20.7024.7589</td>
<td>+1.617.330.4813</td>
</tr>
<tr>
<td><a href="mailto:carol.beaumier@protiviti.com">carol.beaumier@protiviti.com</a></td>
<td><a href="mailto:bernadine.reese@protiviti.co.uk">bernadine.reese@protiviti.co.uk</a></td>
<td><a href="mailto:carl.hatfield@protiviti.com">carl.hatfield@protiviti.com</a></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chetan Shah</th>
<th>Luis Canelon</th>
</tr>
</thead>
<tbody>
<tr>
<td>+1.704.972.9607</td>
<td>+44.20.7024.7509</td>
</tr>
<tr>
<td><a href="mailto:chetan.shah@protiviti.com">chetan.shah@protiviti.com</a></td>
<td><a href="mailto:luis.canelon@protiviti.co.uk">luis.canelon@protiviti.co.uk</a></td>
</tr>
</tbody>
</table>