Avoiding Buyer’s Remorse with AML Monitoring Software

Implementing Effective and Efficient AML Transaction Monitoring Systems
Overview

A well-designed transaction monitoring program is an important pillar of a strong anti-money laundering (AML) compliance program. It supports efforts to combat money laundering and terrorist financing by helping financial institutions identify unusual or suspicious activity that must be reported to regulatory authorities and aids in law enforcement’s tracking and prosecution of criminals involved in money laundering and terrorist financing.

Financial institutions, due to intensifying regulatory scrutiny and a changing geopolitical environment, must constantly update their AML transaction monitoring efforts; therefore, it’s not surprising many are making greater investments in monitoring systems. In 2009 and 2010, financial institutions implemented more than 1,200 new AML transaction monitoring systems.1 In 2010, the global market for AML software was valued at US$450 million and is expected to reach US$650 million by 2015.2

Still, despite the increasing level of investment in AML systems – and the number of personnel dedicated to supporting monitoring functions – AML transaction monitoring efforts in many organizations are suboptimal. This is often because efforts to design AML transaction monitoring programs are deficient from the outset, and/or lessons learned are not incorporated into the program in an appropriate or timely manner.

This white paper examines the consequences of implementing inadequate AML transaction monitoring programs and some of the common myths about monitoring systems. Also discussed are factors management should consider before implementing a monitoring system and issues critical to a successful implementation. Additionally, this paper addresses post-implementation steps for maintaining the AML transaction monitoring system to ensure it remains efficient and effective.

2 Ibid.
TRANSACTION MONITORING SYSTEMS: COMMON MYTHS AND IMPLEMENTATION ISSUES

AML transaction monitoring programs and systems can be evaluated on two scales: effectiveness, the ability of the program and related reports and systems to detect suspicious activity; and efficiency, the ability to minimize the number of alerts generated for non-suspicious activities.

Ideally, a system should detect all suspicious activity (effectiveness) without generating inordinate numbers of false positive alerts that will require time and resources to review (efficiency). Alerts generated should be useful, and allow the financial institution to focus its efforts on investigating activities that are more likely to lead to the identification of potential money laundering or terrorist financing activities.

When evaluating AML transaction monitoring systems, financial institutions must decide on the combination of tools that will work best for their specific risk profiles and tolerances. Tools and technologies run the gamut from standard reports to complex and sophisticated monitoring systems. There are simple, system-generated reports for monitoring suspicious activity involving specific types of products, such as loan prepayment reports. And there are intelligent, automated monitoring systems that not only can be used to monitor multiple types of products simultaneously, but also can adapt over time based on trends identified in historical customer activity and/or peer comparisons.

In addition to the challenge of finding the right blend of AML transaction monitoring tools that meet their particular requirements, financial institutions (most are using some type of technology) must sort through myths and facts about what the technology can and cannot do. These myths have arisen partly due to the proliferation of technology offerings, but also because of organizations’ desire to identify a “silver bullet” solution to meet all of their needs. Below is a list of 10 common myths about AML transaction monitoring systems, examples of vulnerabilities that can arise in the organization if the myths are not questioned, and the facts that organizations ought to know.

<table>
<thead>
<tr>
<th>Myth</th>
<th>Vulnerabilities</th>
<th>Facts</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Technology is the solution to all problems.</td>
<td>The best of systems will not yield the desired results, unless it is used by qualified, experienced individuals.</td>
<td>Technology is just a tool and must be supported by a competent monitoring team.</td>
</tr>
<tr>
<td>2 The “out of the box” solution will work fine.</td>
<td>Monitoring system may not be customized to the financial institution’s unique profile and needs.</td>
<td>“Out of the box” is a template solution that should be configured to meet the financial institution’s unique profile.</td>
</tr>
<tr>
<td>3 All automated monitoring systems are the same.</td>
<td>Financial institutions may choose systems that do not match the complexity of their organization, select a solution with too many features, and/or lack necessary capabilities to perform effective and efficient monitoring.</td>
<td>Automated monitoring systems are designed for a variety of financial institutions. Systems have different functions and modules that are better suited for certain financial institutions.</td>
</tr>
<tr>
<td>4 The most sophisticated and/or most expensive system is the best.</td>
<td>Financial institutions overpay for functions they do not need.</td>
<td>Financial institutions should pay only for system modules that contain functions they need now or anticipate they may need in the near future.</td>
</tr>
<tr>
<td>Myth</td>
<td>Vulnerabilities</td>
<td>Facts</td>
</tr>
<tr>
<td>------</td>
<td>----------------</td>
<td>-------</td>
</tr>
<tr>
<td>5 Our IT department will have no problem implementing and maintaining the system.</td>
<td>The IT department may not understand business requirements for the system or the functionalities of the system. As a consequence, the system is not implemented and maintained as intended by management.</td>
<td>There should be close collaboration between IT and compliance management to ensure business requirements set by management are configured in the system correctly by IT.</td>
</tr>
<tr>
<td>6 The system captures all customers, products, services and geographies.</td>
<td>The system may not be designed to monitor certain areas of the financial institution at all or may not adequately monitor for common “red flag” indicators of suspicious activity.</td>
<td>Pilot testing should be performed during implementation to ensure the system captures all customers, products, services and geographies or that alternate arrangements are made to monitor excluded activities.</td>
</tr>
<tr>
<td>7 The system’s user manual is the monitoring policy.</td>
<td>Regulators, third parties (e.g., auditors) and employees may not understand how the system works or the rationale for how it was set up. Management may not have a document upon which to base future system modifications.</td>
<td>Customized documentation should be created and maintained by the financial institution as it implements and makes modifications to the monitoring system.</td>
</tr>
<tr>
<td>8 Fewer people will be needed for monitoring.</td>
<td>Backlogs of unresolved alerts may develop or the alert reviews may be rushed and quality compromised because of inadequate staff.</td>
<td>The right number of people needed to staff the monitoring team should be determined once the system is in a normalized state.</td>
</tr>
<tr>
<td>9 Once installed, the system will require minimal updating.</td>
<td>The system may not adapt to changes made to the financial institution’s profile and therefore will not continue to monitor all areas of the financial institution.</td>
<td>Periodic reviews need to be performed to adapt the monitoring system to changes in the financial institution’s customer, product, service and geographic profile.</td>
</tr>
<tr>
<td>10 It’s not necessary for the AML compliance department to understand how the technology works.</td>
<td>The AML compliance department will not be able to recommend meaningful enhancements to improve the effectiveness of the technology.</td>
<td>The AML compliance department should understand how the monitoring system detects suspicious activity and the customization that is possible.</td>
</tr>
</tbody>
</table>

**CONSEQUENCES OF MONITORING SYSTEM IMPLEMENTATION ISSUES**

There are tangible consequences of not having up-to-date, properly configured tools to monitor for suspicious activities. Financial institutions may face enforcement actions, civil and criminal penalties, and costly remediation and disruption of business plans. Additionally, financial institutions, and their officers and employees, may face prosecution; individuals may be incarcerated, and corporate and personal reputations may be damaged.
Transaction monitoring programs are commonly cited in AML enforcement actions. A recent, high-impact example of the failure to implement an adequate AML transaction monitoring program involved the assessment of civil penalties of $10.9 million and a Deferred Prosecution Agreement against a U.S. regional bank. The chart below summarizes some of the issues with the bank’s AML transaction monitoring procedures that were cited by the regulators:

<table>
<thead>
<tr>
<th>Transaction Monitoring Issues</th>
<th>Comments</th>
</tr>
</thead>
</table>
| Inadequate review and update of the system | • The bank failed to review and update the filtering criteria and thresholds periodically, which resulted in rules that were not customized to the bank’s current risk profile and the generation of ineffective alerts.  
• Few Suspicious Activity Reports (SARs) were filed by the bank relative to the number of alerts generated. |
| Inadequate coverage of: Red flags | The bank did not monitor the following products:  
• Large, rounded wire transactions in volumes of tens of thousands of dollars  
• Activity inconsistent with company profiles and lacking any apparent lawful business purpose |
| Products | The bank did not monitor for the following red flags:  
• Internal account transfers  
• Automated Clearing House (ACH) transactions  
• Check, loan and trade finance transactions |
| Customers | • Only customers designated as “high risk” (15 percent of the total customer base) were monitored by the system. All other customers were monitored manually, but based on the scope and volume of transaction activity within these accounts, manual monitoring was not sufficient.  
• Domestic and foreign customer accounts were not monitored for frequent high-value rounded wire transactions from Mexican casas de cambio. |
| Backlog of ineffective alerts | At the end of 2006, a backlog of more than 100,000 automated alerts had been generated by the bank’s monitoring system, notwithstanding the fact that only 15 percent of the bank’s customer accounts were being monitored through the automated system. |
| Inadequate system documentation and governance | There was inadequate system documentation to explain account filtering criteria or thresholds and how either was appropriate for the bank’s risks. |

In addition to the large fine, the regional bank in this case spent additional resources for external reviews of AML controls and dedicated significant time and resources over a three-year period to clear a large backlog of alerts produced by an inefficient monitoring system.
To develop an effective and efficient AML transaction monitoring program that will support a financial institution’s specific risk profiles and tolerances, a number of factors should be considered at different stages in the life cycle of the AML transaction monitoring system. The five key stages are:

- **Stage I: Planning** – Developing an understanding of the necessary functionality of the system to be implemented
- **Stage II: Implementation** – Configuring the monitoring system
- **Stage III: Pilot testing** – Testing to understand the effects of the chosen configurations
- **Stage IV: Alert review and trend analysis** – Reviewing suspicious activity alerts generated by the system after it is “live” and identifying trends from alert review that are used to update the AML transaction monitoring system and program
- **Stage V: Maintenance** – Ensuring the system remains efficient and effective in identifying potential money laundering transactions

The following chart depicts the process for developing a new AML transaction monitoring system; a detailed discussion of the five key stages of an AML transaction monitoring system follows.

Before examining the five stages, it is worth offering some insight on system documentation. System documentation is best created as the program and its systems are developed, rather than entirely at the beginning or end of an implementation process. If completed at the beginning, documentation likely will have to be rewritten many times to incorporate changes made during the course of implementation. If created at the end, details may be forgotten and lost.

Complete and accurate system documentation is critical since it allows:

- Management to review and adapt the system for changes in the future
- Users to understand the system while reviewing suspicious activity
- Regulators and third parties to understand how the monitoring program functions
In each stage described below, specific information that should be included in system documentation is addressed.

**Stage I: Planning**

The goal of the planning stage is to define the minimum desired functionality of an AML transaction monitoring system based on the specific profile of the financial institution. The desired functionality of the system should be a primary consideration when assessing vendors and solutions.

**Factor 1: The risk assessment: driver of the transaction monitoring system**

Prior to determining the desired functionalities of an AML transaction monitoring system, management should review the financial institution’s AML risk assessment. This will help establish priorities for monitoring, as well as the features the monitoring system will need to incorporate for the organization’s unique risk profile (i.e., the financial institution’s customers, products, services and geographies).

When selecting a technology solution, financial institutions should address vendor qualifications and capabilities, technical factors, functionality, customer support and cost. Some key characteristics to consider include, but are not limited to, the following:

- **Vendor**
  - How long has the software vendor been in the market? Is the vendor viable?
  - What experiences have other financial institutions had with the vendor and its software solutions?
  - Is the vendor knowledgeable about regulatory requirements?
  - For international financial institutions, is the vendor able to provide services on a global basis (e.g., multilingual capabilities)?
  - Is the system an enterprisewide solution across business lines (e.g., bank, broker-dealer and insurance)?

- **Technical factors**
  - Will the system be able to monitor all customers and products? If not, how significant are the exceptions?
  - Does this system offer standardized rules and scenarios? How much customization will be required to adapt the rules to the financial institution’s unique risk profile?
  - Is the system scalable in terms of transactions and customers?
  - What security features does the system have (e.g., controls)?
  - Does the solution provide a detailed audit trail?
  - Will the installation require significant customization (e.g., data feeds, parameters)? If so, to what extent and how will it impact the implementation and costs of the system?
  - How are upgrades delivered to the financial institution?
  - Is the software compatible with the organization’s existing hardware or will additional hardware need to be purchased?
• **Data**
  – How useful and accessible is the financial institution’s data?
  – How much data cleanup (e.g., validating accuracy of transaction codes, linking related accounts) will be required to optimize the use of the AML transaction monitoring system?

• **Customer support**
  – Is the software user-friendly (e.g., is the graphical user interface [GUI] easy to learn)?
  – How frequently is the vendor committed to upgrading the software? How quickly does the vendor make changes to address new areas of concern?
  – How are upgrades implemented?
  – Does the vendor provide training (initial and ongoing)?
  – Does the vendor assist financial institutions with customizing the system?

• **Cost**
  – What pricing model (e.g., per user, site license, transaction volume) is offered by the vendor?
  – Is implementation included in the cost of the system?
  – Is ongoing customer support included in the cost of the system?
  – Are upgrades included in the cost of the system?
  – How will use of the system affect the number of people the financial institution needs for monitoring?

As noted earlier, no “out of the box” monitoring system is likely sufficient to address all of a financial institution’s specific needs. To be effective, most systems will need customization. Therefore, when comparing AML transaction monitoring systems, an effective approach for financial institutions is to develop a scorecard that rates various systems based on needed and desired functionality (the “must haves” and the “nice to haves”). These documented scorecards also provide evidence of the due diligence process that the financial institution undertook to select the technology.

**Factor 2: Data feeds and integrity**

For rules in automated transaction monitoring systems to cover the different areas in a financial institution, complete and accurate data must be available for the systems. AML compliance staff should collaborate with IT staff to evaluate data integrity by ensuring:

• Core systems are completely capturing all transactions

• Core systems have transaction codes to differentiate between different transaction types for each product and service type (e.g., incoming wire transfers, deposits of monetary instruments)

• Data from core systems can be extracted and fed into monitoring systems accurately and completely
Where data feeds are not part of the financial institution’s core system and cannot be loaded into the automated transaction monitoring system, AML compliance staff will need to monitor these areas with supplemental monitoring reports. Examples of where this may occur include the processing of certain customers or products on isolated platforms; services that cannot be monitored with automated systems (e.g., trade finance); products that require manual, detailed review (e.g., omnibus accounts); and monitoring for specific activities that cannot be detected through automated system monitoring (e.g., human trafficking).

Ultimately, the combination of automated and manual monitoring methods should provide coverage for all areas of the financial institution. Financial institutions also should determine whether client profile information can be extracted and fed into customer due diligence modules in the AML transaction monitoring system. This will enable monitoring to be centralized into one system, allowing the monitoring team to review suspicious transactions and customer information in one system.

**Documentation Tips**

At the end of Stage I, management should review the evaluation scorecard used to determine how the financial institution’s needs will be met by the monitoring system’s functionality, and then adjust documentation accordingly. The scorecard should describe the different customers, products, services, and geographies that need to be monitored for money laundering, highlighting areas with the highest AML risk. Given the availability of data feeds for each area, the documentation should show how the system (or supplemental monitoring reports) covers all areas of the financial institution, highlighting again how the highest risk areas are being covered.

**Stage II: Implementation**

The goal of the implementation stage is for the financial institution to create settings and define reports for AML transaction monitoring systems by choosing specific rules to be monitored.

**Factor 1: Rule selection**

Once an automated system is selected, it must be customized to the financial institution’s specific needs. This means selecting the rules – the logic – that will be used to develop alerts. Management should not allow vendors to decide which rules are appropriate for their financial institution. Additionally, they should independently verify that the rules are appropriate for their operations and will produce meaningful alerts.

To select effective rules, management should consider the following factors:

- **Coverage of common red flags**

  The Federal Financial Institutions Examination Council (FFIEC) has developed common red flags for potentially suspicious activity. There are red flags for customers, services and products. Not all flags will be applicable to every financial institution, but it is important for management to make a deliberate and informed decision on which are necessary. Rationale for any coverage gaps should be documented so regulators can understand why full coverage is not necessary given the financial institution’s activities and risk profile.
• **Account/customer/peer group comparisons**

AML transaction monitoring systems identify activity that is out of the ordinary and potentially suspicious. One way to develop baseline activity considered “normal” is to compare current activity to historical activity. Historical activity can be collected on an account, customer or peer group level, and rules can be developed to generate alerts when current activity exceeds historical activity at significant levels. Alternatively, expected activity information collected during customer on-boarding due diligence can be used to develop baseline activity until sufficient historical activity has been collected.

• **White lists**

Financial institutions also may consider the use of “white lists” to increase the efficiency of monitoring systems. White lists include accounts excluded from some or all monitoring regimes; examples include internal and operating accounts, such as a financial institution’s payable or receivable accounts.

White lists also may be developed for specific rules. For example, for a “flow through of funds” rule – when the financial institution is flagging accounts where money is flowing in and almost immediately flowing back out – account types such as payroll accounts may be white-listed.

Overuse or inappropriate use of white lists can result in legitimately unusual or suspicious activity being missed. Therefore, to ensure that the effectiveness of the AML transaction monitoring system is not compromised, it is important for financial institutions to have strong documentation to explain the inclusion of accounts on white lists.

**Factor 2: Determination of rule parameters**

Once the list of rules is established, the financial institution will need to set the initial parameters for each rule. Here again, the parameters provided by the vendor should not be used “out of the box” without review and validation by the financial institution.

For rules that cover common red flags, especially FFIEC-identified red flags, regulatory thresholds can be used (e.g., Bank Secrecy Act reporting requirements for cash activity). For rules that perform account, customer or peer group comparisons, statistical analysis can be used to determine appropriate value and volume deviation limits. Standard deviation analysis can be performed on the account, customer or peer group data to identify the level of activity that is “normal.”

The financial institution also can determine parameters by developing worst-case scenarios for customer activity for products, services and geographies. Based on the financial institution’s risk appetite, management can define a level of activity that is allowed to occur without an alert being necessary. Parameters can then be set based on this level of activity.

As an example, a financial institution may decide that particular groups of business customers can send wires to high-risk jurisdictions each month without an alert being generated. This may be determined because due diligence and historical activity on these business customers have shown they perform legitimate international transactions in high-risk areas.
However, if parameters for high-risk wire transaction rules were set lower, the system would be inefficient because it would generate recurring false positive alerts on what is actually normal activity for a particular type of customer. As with white lists and other rules that exclude certain activities or customers from alert generation, thresholds should be periodically reviewed and validated to ensure they remain appropriate.

**Documentation Tips**

Once Stage II is complete, management should document the specific parameters that are in place to monitor the products, services and customers of the financial institution for suspicious activity, including exceptions made for certain customers. The rationale for choosing rules and their specific parameters, based on risk appetite, statistical analysis and regulatory guidance, should be explained.

**Stage III: Pilot testing**

The goal of pilot testing is to determine how the system will perform before it goes “live.” During this phase, the system can be evaluated to determine whether it is flagging transactions as intended and whether the financial institution is prepared to handle the volume of alerts that will be generated.

**Factor 1: Pilot testing of settings**

Pilot testing of settings for the AML transaction monitoring system should, at minimum, include the following activities:

- Comparison of alerts flagged by the system to activity included in the financial institution’s previous SAR filings to ensure areas of known risk are being flagged.

- Evaluation of the utility of the alerts being generated to determine whether additional modifications might eliminate false positives without undermining the integrity of the monitoring effort. Common root causes for false positives include:
  - Faulty data feeds.
  - Duplicate alerts being generated by two or more rules. This can happen when rules have overlapping parameters. For example, if rules are created to flag wire transfer activity between $10 million and $40 million, and also between $35 million and $50 million, then duplicate alerts would be generated for activity between $35 million and $40 million.

- Comparison of system output to a current system for categories of activity where the new implementation represents an upgrade and not an initial installation.

Additionally, management should assess whether existing staff can handle the number of alerts the system is expected to generate once stabilized. More personnel may be needed to prevent backlogs from forming in the AML transaction monitoring system.
Factor 2: Determination of final thresholds for rules

After pilot testing is complete, the AML transaction monitoring team can finalize thresholds and rules. During this process, the team should take a conservative attitude toward finalizing thresholds; further tuning of the system can be performed later. It is preferable, notwithstanding the effect on the monitoring team, to create inclusive thresholds that generate more alerts when a system is launched, rather than risk missing suspicious activity.

Documentation Tips

At the end of Stage III, management should finalize the rules and parameters in the AML transaction monitoring program documentation. Management may also document the results of pilot testing to continue tracking changes made to the monitoring system. Additionally, in this phase, management should assess and then document both the organizational structure of the AML transaction monitoring team and the relevant skills and experience they possess to review correctly activity flagged by the monitoring system.

Stage IV: Alert review and trend analysis

This stage captures the day-to-day activities of the monitoring team and, in some financial institutions, analysts who work with the data developed by the monitoring team to identify trends that can be used for tuning both the monitoring system and the program as a whole.
Factor 1: Analyzing monitoring system trends for tuning opportunities

As the system generates alerts that are reviewed by the AML transaction monitoring team, trends emerge. These patterns, once identified, offer opportunities for improving the effectiveness and efficiency of the system. Trend identification by frontline users of the system is one of the sources of feedback that financial institutions should consider when performing periodic tuning of the system. Below are some areas that financial institutions should analyze for trends and system-tuning opportunities:

- **Reviewing alert-to-case ratios**
  A high percentage of alerts escalated to cases are a sign a rule is efficient and effective. Cases indicate there is potentially suspicious activity and require additional review by the monitoring team before they are cleared or escalated again for SAR filings. Financial institutions should review any rules that have low alert-to-case ratios to understand whether parameters should be adjusted to lower the “false positives” (the number of alerts cleared without escalation). A low ratio may indicate there are problems with data feeds flowing into the transaction monitoring system or that staff are insufficiently trained (see point below, “Identifying areas for training”).

- **Identifying factors contributing to cases/SAR filings**
  Similar to reviewing alert-to-case ratios, identifying the factors contributing to cases and SAR filings may allow a financial institution to increase the efficiency and effectiveness of its monitoring system. Analyzing cases and SARs to understand which products, services, customers or geographies appear most frequently allows the financial institution to ensure adequate resources continue to review the true positive alerts for suspicious activity in those areas. For areas with few cases or SAR filings, the financial institution may again review parameters, data feeds and staff training to reduce the number of false positives the AML transaction monitoring team must review.

- **Identifying areas for training**
  As noted earlier, alerts may not be escalated to cases because the monitoring staff is not trained adequately to identify suspicious activity. To ensure alerts are reviewed correctly, additional quality control reviews of cleared alerts by more experienced staff can be conducted. Conversely, too many cases may be opened by staff members who have less experience and may choose to err on the side of caution. Additional quality control reviews or targeted red flag training for specific products or services may be a solution if the team is escalating many alerts for a particular rule.

- **Reviewing cases/SAR filings generated outside of automated monitoring**
  Cases and SAR filings may arise from other sources at the financial institution, including internal referrals from frontline employees such as tellers and customer relationship managers. Repeat cases and SAR filings from these sources may indicate new rules should be implemented to ensure there is automated monitoring for these areas. Non-system sourced cases and SAR filings also may indicate new trends and red flags for money laundering.

- **Detecting duplication of alerts output**
  Some rules may generate alerts on the same activity, causing lower efficiency because multiple alerts will have to be reviewed; this often happens after AML transaction monitoring systems go through cycles of change and updating. If duplicate alerts are being generated, some rules should be eliminated to prevent growing backlogs of false positive alerts. If backlogs occur, management should determine the root causes; in addition, strategies should be developed to address how to reduce backlogs (e.g., high-risk customer alerts reviewed first).
Stage V: Maintenance of the transaction monitoring system

The goal of maintaining the AML transaction monitoring system is for the financial institution to ensure it continues to be efficient and effective in identifying money laundering transactions. This is accomplished by ensuring the system and the risk assessment adapt to changes in the financial institution’s profile. The system also should be improved based on the trends identified during trend analysis.

The chart above depicts the cyclical process of maintaining the transaction monitoring system. It begins with the clearing and escalating of alerts from the system. As part of this process, trends are identified, which can be used to both update the monitoring system and the risk assessment. Additionally, the risk assessment should be updated to reflect changes in the financial institution’s profile.
**Factor 1: Updating of the risk assessment**

As early as six months after implementation (and at least on an annual basis), financial institutions should review the AML transaction monitoring systems that were implemented. These reviews will enable financial institutions to increase efficiency of the system and ensure the overall AML transaction monitoring program mirrors any fundamental changes made at the financial institution.

The risk assessment should be reviewed and updated in conjunction with the monitoring system because it is the driver of the AML transaction monitoring program. Trends that emerge from the AML monitoring system and profile changes at the financial institution should be included when updating the risk assessment:

- **Validation of risk assessment using monitoring system trends**
  - The risk assessment should be validated by the outputs of the transaction monitoring system. For areas identified as high risk by management in the risk assessment, there should be more alerts, cases and SARs filed. Statistics, such as the alert-to-case ratio and frequency of product, service, customer or geography appearance in cases and SARs, can be added to risk assessment documentation to support management’s decision to designate certain areas as high risk. These statistics also may be used to support the change in risk ratings of other areas.
  - In addition to validating the risk assessment, AML transaction monitoring can identify new trends in money laundering, which can lead to the development of new red flags and change the risk levels of certain areas of the financial institution.

- **Input from profile change of the financial institution**
  - Changes in the financial institution’s customers, products, services and geographies of operation should be reflected in the risk assessment. Changes can include adding new products or services, modifying policies to allow for non-customer use of certain products and services, or starting new operations in different geographies. Rationale should be provided based on the financial institution’s profile for risk ratings that are added for new areas.

**Factor 2: Monitoring system-tuning trends**

The identified trends noted in Stage IV can be used to update the AML transaction monitoring system to ensure continued efficiency and effectiveness. Parameters for individual rules can be adjusted to increase the number of true positives that are identified by the system. Rules may be added or removed depending on holes in coverage that are found, or if there are duplicative alerts generated:

- **Updating the monitoring program**
  - If changes need to be made to the AML transaction monitoring system parameters, test environments should be used to understand the effects of the changes before they are applied to the live environment. Effects in terms of level of alerts generated should be considered to understand whether additional staff will be required to review additional alerts. Also, because tuning of the system will be performed on a regular basis, changes should be made gradually to thresholds. Future rounds of tuning will provide updated feedback for additional improvements to the system.
• **Adding rules to the monitoring system**
  If the financial institution is exposed to new products, services, customers or geographies, new rules and parameters will need to be developed for the system. Any newly identified trends in money laundering also require the implementation of new rules. The risk assessment and risk appetite should once again drive the rules and parameters that are set.

• **Making adjustments to the monitoring system based on risk rating changes**
  If risk ratings change, the level of monitoring may be adjusted within the AML transaction monitoring system through changes to parameters for rules. Areas changed to higher risk ratings will require adjusting thresholds to allow the AML transaction monitoring system to capture more of the activity from the area, so the activity can be reviewed by the monitoring team.

• **Making adjustments to policies and procedures and the monitoring team**
  The governance and resources that support the AML transaction monitoring system also may need to be revised. Policies and procedures, including the timelines for clearing of alerts and quality control, may be tweaked after analyzing the monitoring system trends. Training and hiring of more experienced staff may also be solutions for issues identified during monitoring trend analysis.

**Documentation Tips**
At the end of this last stage, management should have established and documented policies and procedures for maintaining the AML transaction monitoring system. The policies should state how often reviews will be completed for the risk assessment and the monitoring system. Also, responsibility for performing reviews, recommending changes, and approving changes to rules and parameters should be assigned to appropriate staff.

**IN CLOSING**

An AML transaction monitoring system is an important tool in a financial institution’s anti-money laundering program and must be customized and maintained. Management should not view the monitoring system as a static tool that is set up at the time of purchase to generate alerts until it is replaced by the next system. Instead, the system should be viewed as a dynamic tool that evolves alongside the financial institution as it changes and grows. Taking a proactive approach to customizing and maintaining the system will allow the overall program to be effective and efficient in detecting money laundering, thus saving the financial institution from costly fines, regulatory actions and reputational damage.
Protiviti (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® 1000 and 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 International Inc. (NYSE: RHI). Founded in 1948, Robert Half International is a member of the S&P 500 index.

How Protiviti can help

Whether your financial institution is implementing an AML transaction monitoring system for the first time, changing vendors and systems, or performing periodic review and maintenance of current systems, Protiviti has the experience and resources to help. Below is a short summary of how we can assist your financial institution in each of the five stages discussed in this white paper.

<table>
<thead>
<tr>
<th>Stage</th>
<th>Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>Planning</td>
<td>• Review to ensure program is risk-based</td>
</tr>
<tr>
<td>Implementation</td>
<td>• Review data feeds and data integrity</td>
</tr>
<tr>
<td></td>
<td>• Assist in the development of rules and parameters</td>
</tr>
<tr>
<td>Pilot testing</td>
<td>• Review to ensure policies and procedures are appropriate</td>
</tr>
<tr>
<td></td>
<td>• Review to ensure management/users have adequate knowledge</td>
</tr>
<tr>
<td></td>
<td>• Provide training to end users and refresher training for management</td>
</tr>
<tr>
<td></td>
<td>• Perform pilot testing to understand whether initial parameters for rules are effective/efficient</td>
</tr>
<tr>
<td>Alert review and trend analysis</td>
<td>• Evaluate system configurations using worst-case scenarios</td>
</tr>
<tr>
<td></td>
<td>• Evaluate system for adequate coverage of financial institution’s profile</td>
</tr>
<tr>
<td></td>
<td>• Provide support to clear accumulated backlogs</td>
</tr>
<tr>
<td>Maintenance of the monitoring program</td>
<td>• Provide recommendations for improving system effectiveness and efficiency based on changes at financial institution</td>
</tr>
<tr>
<td></td>
<td>• Assist in the validation of risk assessment based on monitoring system trends</td>
</tr>
<tr>
<td></td>
<td>• Perform periodic reviews of the monitoring system</td>
</tr>
</tbody>
</table>
For additional information about the issues reviewed here or Protiviti’s services, please contact:

Carol Beaumier  Andrew Clinton
Managing Director  Managing Director
+1.212.603.8337  +44.207.024.7570
carol.beaumier@protiviti.com  andrew.clinton@protiviti.co.uk

Shaun Creegan  Bernadine Reese
Director  Managing Director
+1.212.708.6362  +44.20.7024.7589
shaun.creegan@protiviti.com  bernadine.reese@protiviti.co.uk