AML/CFT Transaction Monitoring: Alert-Based Monitoring vs Case-Based Monitoring

By: Terence Ho
Contents
1. Executive summary: .............................................................................................................3
2. Introduction ..........................................................................................................................5
3. Issues arising from Transaction Monitoring .................................................................6
4. Transaction Monitoring: Alert Based and Case Based ....................................................8
5. Comparison Between Alert-Based Monitoring and Case-Based Monitoring ..............10
6. Case Example .....................................................................................................................14
7. Conclusion .........................................................................................................................15
8. Works Cited .......................................................................................................................16
1. Executive summary:

Over the years, U.S. regulatory agencies such as the Financial Crimes Enforcement Network (FinCEN), the Office of the Comptroller of the Currency (OCC) and the New York State Department of Financial Services (NYDFS) have been actively issuing consent orders against financial institutions that have failed in their responsibility to identify, detect, and report suspicious transactions. Some of the financial institutions that have been singled out specifically for deficiencies in transaction monitoring efforts include Wachovia Bank N.A. (2010),¹ HSBC Bank USA N.A. (2012)² and Commerzbank AG (2015)³ with fines aggregating to more than $3.5 billion to settle the allegations.

Outside of the U.S., regulators in major financial centers such as London, Hong Kong and Singapore have demonstrated strong commitments in maintaining the integrity of the country’s respective financial systems in recent years.

In an enforcement action on October 12, 2016, Mark Steward, the Financial Conduct Authority’s (FCA) director, said that “Fighting money laundering is an issue of extreme international importance and ensuring that AML controls are effective and viewed as important throughout the business are fundamental obligations of all regulated firms.”⁴

On July 31, 2015, the Hong Kong Monetary Authority (HKMA) took its first disciplinary action against a financial institution for AML failures. Director-General (Enforcement) of the HKMA Meena Datwani said, “The HKMA takes such failures seriously and wants to send a clear message to the industry that all authorized institutions should have effective AML/CFT systems and controls in place to, among other things, detect and report suspicious transactions based on their knowledge of their customers.”⁵

¹ From the OCC News Release of March 17, 2010
² From FinCEN Assessment of Civil Money Penalty of December 10, 2012
https://www.fincen.gov/sites/default/files/enforcement_action/HSBC_ASSESSMENT.pdf
³ From the New York State Department of Financial Services Press Release of March 12, 2015
http://www.dfs.ny.gov/about/ea/ea150312.pdf
⁴ Remarks of Mark Steward, Director, Financial Conduct Authority
⁵ Remarks of Meena Datwani, Director-General, Hong Kong Monetary Authority
On October 11, 2016, a merchant bank was fined S$4.3 million and ordered to cease operations by the Monetary Authority of Singapore (MAS) for “serious failures in anti-money laundering controls and improper conduct by senior management.” Ravi Menon, managing director at MAS, said, “[Financial institutions] must put in place robust mechanisms to detect suspicious activities... MAS will ensure that standards are kept high and will take strong deterrent actions against institutions that fall short.”

Financial institutions are increasingly expected to fulfill their transaction monitoring obligations as part of its overall effective anti-money laundering (AML) programs and the regulators are showing no signs of slowing down on enforcement actions against errant institutions. Some of the findings from the regulators include:

- “[The institution] … did not have an adequate number of employees or sufficiently experienced personnel.” (NYDFS³)
- “[The MLRO] … failed to impress upon senior management the need for more resources in the MLRO function and failed to take adequate steps to recruit more staff in a timely fashion.” (FCA⁴)
- “Inadequate scrutiny of customers’ transactions and activities, and failure to file timely suspicious transaction reports.” (MAS⁵)

The trend seems to suggest that financial institutions are encountering difficulties in managing the appropriate staffing levels and level of scrutiny in customer’s transactions. While the appropriate staffing level should be determined by the risk level of the bank’s products and services, the level of scrutiny into the customer’s transactions can be more effectively handled by employing a risk-based approach to managing the alerts generated by the monitoring systems on an account-level basis. This can be achieved by aggregating the generated alerts on a customer level basis and ensuring customers with the highest perceived risk scorings get the required attention over others, which are deemed to be of a lower risk.

This white paper provides an alternative approach to handling alert-based monitoring systems to better enable concentration and efficient use of precious AML expertise in the financial institutions.

---

⁶ Remarks of Ravi Menon, Managing Director, Monetary Authority of Singapore
2. Introduction

After the terrorist attacks on September 11, 2001, government bodies around the world reacted swiftly by enacting new laws to criminalize money laundering and terrorist financing, provided regulatory guidance as well as stepping up on supervisory and enforcement actions on financial institutions whom are viewed as important allies in the prevention of money laundering. The enactment of the USA PATRIOT Act in the U.S. on October 26, 2001, the record fine imposed on HSBC Holdings Plc on December 10, 2012, and the formation of dedicated departments to combat money laundering by the MAS in August 2016⁷ are testaments of the commitments of the various governments to deter reckless and wilful blindness behavior in the industry.

Often during inspections, regulators assess whether the AML program of the institution is effective and ensure that the standards are kept high. Transaction monitoring, which is an important part of a solid AML program, requires consideration on various factors such as:

- Size of institution
- Jurisdictions in which the institution operates
- Type of business activities
- Types of transactions in which its customers engage

A report by Capgemini⁸ and BNP Paribas estimated that the total number of non-cash transactions in 2015 stood at 426.3 billion.⁹ Assuming Pareto principle holds, the top 20 percent of the largest financial institutions in the world would have cleared 80 percent of the total number of wire transfers annually. The number of wires (341 billion) passing through these large banks would hence be close to 30 billion each month. Further assuming the top 20 percent of the largest financial institutions stood at 3,000 and we have a transaction to alert the conversion rate of 1 percent, each financial institution would on average, potentially face up to 100,000 AML alerts arising from 10 million wire transfers to review each month. Of course, the above figures are based on multiple assumptions which may vary greatly depending on the various factors mentioned in the previous paragraph. Nevertheless, from the FinCEN

---

⁷ Press release by the Monetary Authority of Singapore, 13 June 2016
⁸ Capgemini is a consulting firm <https://www.capgemini.com/>
⁹ 2016 World Payments Report by Capgemini and BNP Paribas
https://www.worldpaymentsreport.com/reports/noncash
Assessment of Civil Money Penalty of HSBC in 2012,\textsuperscript{2} it was revealed that the multinational institution “…processed an average of approximately 25 million wire transfers annually.”

3. Issues arising from Transaction Monitoring

With large financial institutions processing enormous volumes of transactions each day, the corresponding number of AML alerts generated would equally be unmanageable if steps are not taken to ensure staff proficiency as well as alert efficiency. While some financial institutions rely on in-house systems to suit their individual transaction monitoring needs, others prefer to get off-the shelf monitoring systems from vendor providers, which are mostly built on an alert-based monitoring strategy. Alert-based monitoring is an approach commonly deployed to help users manage large volume of data, spot predefined patterns and draw human attention to certain anomalies in areas not just restricted to AML monitoring. Some of the common issues faced by financial institutions on alert based monitoring today include:

- **Overwhelming backlog of alerts**
  
  A backlog of alerts may occur for multiple reasons such as inadequate manpower, inexperienced AML staffs, improperly tuned scenarios, etc. In the hearing of the same case on HSBC by the U.S. Senate,\textsuperscript{10} it was revealed that “the compliance team was “handling an average of 3,800 alerts per person and was becoming overwhelmed thus potentially placing the business and the bank at risk.” The same report highlighted that “OCC examinations also routinely identified inadequate staffing as a key AML problem, including with respect to unreviewed alerts.”

- **Individual employee behavior**
  
  In the case of Commerzbank AG, it was revealed in the NYDPS press release\textsuperscript{3} that a vice president of the bank reported that “the goal of the threshold setting process was set based on a desire not to generate too many alerts… Both the Head of Regional Compliance and the Head of AML Compliance asked him to change the thresholds in the automated system to reduce the number of alerts generated.”

- **Low value alerts**

\textsuperscript{10} United States Senate hearing on HSBC Case History, July 17, 2012
According to an AML survey\textsuperscript{11} by EY in 2014, Securities Brokerage and Corporate Banking businesses have SAR conversion rates as low as 1 percent and alerts worthy of investigation as low as 5 percent. These low value alerts take up precious bank resources that could otherwise be deployed on more SAR-worthy investigations.

- **System suitability**
  The same AML survey by EY in 2014 found that about 60 percent of the respondents felt that vendor-built scenarios only partially met their monitoring needs. Each financial institution varies greatly by the size, customer base, jurisdictions in operation and the type products and services offered. It is highly unlikely that a one-size-fits-all monitoring system could be effectively deployed in every financial institution that purchased the system.

Interestingly, the EY AML survey found that while respondents use a variety of vendor-supplied transaction monitoring systems, some respondents were utilizing more than one vendor system in the financial institutions.

\begin{figure}
\centering
\includegraphics[width=\textwidth]{chart.png}
\caption{Vendor system usage, AML Transaction Monitoring: A Survey of UK Financial Institutions, September 2014}
\end{figure}

\textsuperscript{11} AML Transaction Monitoring: A Survey of UK Financial Institutions, September 2014
The finding by EY seems to suggest that having more than one vendor system in the institution would create synergies, provide better alert coverage and hopefully reduce the risk of missing suspicious transactions.

The same concept can be applied to the review of AML alerts, which are usually limited to highlighting transactions performed in a single account belonging to a customer (i.e., account-level review). When a customer, such as a multinational corporate, has multiple accounts with the bank across several jurisdictions, these alerts should be reviewed simultaneously on a customer level basis by aggregating all relevant alerts generated from the various accounts of the customer (i.e., customer level review) and creating a case for review. In fact, a customer level review is a consolidated review of all alerts associated with the customer’s accounts that were generated during a specified period. The consolidated review provides a holistic overview of the overall customer activity and allows for a more efficient and accurate deployment of resources.

4. Transaction Monitoring: Alert Based and Case Based

Consider the scenario: You are planning to get a new pair of pants for the important dinner that you will be attending this weekend. You have two options: (1) purchase it off-the-rack from a departmental store, or (2) go to a tailor and get your measurements done.

Depending on a variety of factors, some may choose the first option because it is fuss-free and requires less investments in time and money. Others may choose option two because chances are that ready-made products will not fit perfectly because we come in different shapes and sizes.

Financial institutions in the industry face the same dilemma when deciding on the type of transaction monitoring system to implement. While the purchase of an alert-based monitoring system is the most straightforward way out to pass a regulatory exam, they usually come with a huge percentage of low value alerts (false positives) and finding a truly suspicious alert is akin to finding a needle in the haystack. On the other hand, financial institutions may consider building in-house scenarios or a case management system where the scalability and performance of the system can be tailored exactly to the needs of the business to reduce the false positives.

Alert-Based Monitoring
Most financial institutions tend to rely on third-party vendor systems, which monitor transactions based on a standard set of rules, scenarios and statistical models which lead to alert generation. Depending on the internal procedures of the financial institutions, each of these alerts will be assigned and reviewed by a junior analyst before closing it without further action or escalating it to the second level for more in-depth investigations. Once the transactions highlighted by the alert is deemed suspicious, the alert may be closed with a SAR decision or further escalated to the MLRO.

**Case-Based Monitoring**

When analyzing the account activity of a customer with high volume of transactions, most AML professionals rely on data manipulation to make sense of the transactional pattern. Pivot tables are especially useful to consolidate and present information in a summarized manner, identifying who is the largest contributor of payments and the frequency of transfers.

Similarly, the concept of case-based monitoring is to monitor transactions on a consolidated manner instead of individual alerts. In a case-based monitoring setup, alerts generated by the monitoring systems are not immediately reviewed by an analyst. Instead, these alerts are assigned with a risk score and moved into a case file waiting for further consolidation of alerts, which belong to the same customer level group. Once the case has accumulated enough alerts (either by scoring system or by a manual alert override), the case on the customer will be generated and an analyst would be assigned to review the case.

Suppose a financial institution has deployed multiple monitoring systems across its lines of businesses. It has purchased monitoring systems from Vendor A, which has scenarios specialized for retail banking; Vendor B which is effective for brokerage trade monitoring; some customized in-house scenarios for specific products of the bank; a system where employees can file referrals of suspicious activity detected during their daily work and from media report monitoring.

To integrate all these alerts from the different lines of businesses together, the in-house developers need to design a case management system to process these alerts according to its inherent risk score of each scenario as determined by the institution. The alert consolidation
stage will group same parties into a single case or parties that are related through party householding (See Figure A).

Customer activity that has been deemed as not suspicious could be entered back into the case management system via a feedback loop that will suppress or reduce the scoring of similar alerts generated in the future. This would contribute to the reduction of false positives through human intelligence in addition to the standard rule tuning process in an alert-based monitoring set up.

5. Comparison Between Alert-Based Monitoring and Case-Based Monitoring

As mentioned previously, a financial institution may consider deploying an alert-based monitoring system or a case-based monitoring system based on the size and risk of its businesses. The benefits and limitation of both methods are examined below.

Benefits of Alert-Based Monitoring

- **Straightforward review of highlighted transactions.**
  
  Each alert on a customer or account is confined to the scenario and the specific lookback period. Unless the initial assessment of the transactions highlighted is suspicious,
it is usually not necessary to conduct a further in-depth review of the customer’s account.

- **Speed of review**
  According to LexisNexis Risk Solutions True Cost of AML Compliance APAC Survey Report,\(^\text{12}\) 61 percent of the respondents were able to clear an AML transaction monitoring alert within one business day (less than eight hours).

- **Alert thresholds can be easily tuned**
  Alert-based transaction monitoring scenario thresholds can be easily tuned by business or compliance. They do not require programmers to raise a request for a fix which will only be rolled-out on the next release.

### Limitations of Alert-Based Monitoring

- **Large number of false positives**
  When scenarios are not properly tuned, a large number of false positives will be generated, forcing AML analysts to spend long hours looking at low-value alerts. The extended period low-value activity has a negative impact on the skills, morale and enthusiasm of the analysts, leading them to make poor decisions from the investigations.

- **Alert review does not tell the whole story**
  Depending on the type of scenario, an alert typically highlights activity ranging from a day and up to a month. Sometimes, reviewing a month’s worth of transactions may not be sufficient to determine whether the activity reviewed is suspicious. In most circumstances, the analyst is required to further review prior account activity or revisit the account again the following month.

- **Myopic view of the activity**
  Multinational companies that have business operations around the world tend to open business relationships with large financial institutions due to the wide network of banking subsidiaries available. However, an alert-based monitoring system is unable to effectively consolidate cross-border transactions into a single meaningful analysis.

---

\(^\text{12}\) LexisNexis® Risk Solutions True Cost of AML Compliance APAC Survey Report
Challenges

Increasingly, it is not enough to ascertain the legitimacy of transactions highlighted by a single alert. The inherent simplicity of the alert-based monitoring model means that a customer engaged in frequent ‘normal’ inter-company transfers would unlikely get picked up as a set of round tripping transactions with no real business purposes. Similarly, the lack of connection between each individual alert review poses a significant challenge in piecing together a complete story of the customer’s activities.

Benefits of Case-Level Monitoring

- **Holistic review of customer’s activity**
  Implementing a case-based review allows the consolidation of different alerts generated on customers under the same family/household. This will allow a multi-jurisdictional review of the customer, which provides a better understanding of the customer’s behavior

- **Consistent approach in AML monitoring and review**
  The review of transactions across multiple jurisdictions in a single exercise provides a standardized approach in AML investigations across different reporting legal entities of the financial institutions. According to the ‘Sound management of risks related to money laundering and financing of terrorism’ guidelines published by Bank for International Settlements, 13 “each group should develop group-wide AML/CFT policies and procedures consistently applied and supervised across the group.”

- **Allows greater flexibility in risk based approach**
  A case-based monitoring approach ensures that customers with a higher percentage of risk scoring alerts to be prioritized and generated into a case for review. Customers that have a low number of alerts generated may not reach the sufficient threshold to be created into a case, hence reducing the need to review based on a risk-based approach. However, certain parameters such as a referral event would override the alert consolidation and “force” the case to be generated out for review immediately.

---

13 Sound management of risks related to money laundering and financing of terrorism by BIS
http://www.bis.org/bcbs/publ/d353.pdf
referral event can be manually created by any employee of the bank whenever suspicious activity is detected, such as negative media reports, wire-stripping queries by customers, enquiries from law enforcement agencies, grand jury subpoenas, etc.

**Limitations of Case-Level Monitoring**

- **Highly complex**
  The building of a customized case-based monitoring system in-house is a long term and highly complex plan that would require significant investments into technology, infrastructure and human resources. Due to the multiple monitoring systems deployed in the setup, the data in the respective alerts needs to be standardized into a single source feed which would allow meaningful consolidation into case.

- **Suspicious transactions may not get reviewed immediately**
  Due to the nature of the case-based monitoring setup, a case will only be generated for review when certain conditions are met. However, it may be more than a few months before the customer accumulates enough alerts to form a case, hence creating a lag time between transaction date and review date.

- **Requires more time for review**
  Case review turnaround takes a significantly longer time due to the consolidation of multiple alerts. The analysts also require a longer time to complete investigations due to requirements of deeper understanding of the various systems and local regulations of the cross jurisdictional review, which the case might entail.

**Challenges**

Apart from the large initial investments into technology that would be required, many countries have different reporting timelines, which mandate the reporting of suspicious transactions within a specified timeframe (e.g., Philippines require suspicious transactions to be reported by five working days\(^\text{14}\)). The lapsed time between the transaction date and the actual review date may lead to a delay in filing a SAR to the relevant authority. This would require the head of compliance of the financial institution to effectively explain and convince the regulator of the overall AML strategy and the benefits of a case-based monitoring system.

\(^{14}\) Circular Letter No.CL-2016-065 by Banko Sentral Ng Pilipinas, July 20, 2016

6. Case Example

A corporate customer with three accounts with the bank was highlighted by nine monitoring alerts between August 7, 2015 and April 12, 2016. The nine alerts are being consolidated into a case and generated for an analyst to review (see Table 1).

<table>
<thead>
<tr>
<th>Alert type</th>
<th>No of Events</th>
<th>Oldest Alert Date</th>
<th>Latest Alert Date</th>
<th>No. of Trans</th>
<th>No of Accs</th>
<th>Alert Total (USD)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aggregated Cash Withdrawals</td>
<td>2</td>
<td>07 Aug 2015</td>
<td>07 Mar 2016</td>
<td>79</td>
<td>1</td>
<td>55,999.36</td>
</tr>
<tr>
<td>Structured Debit Wires</td>
<td>5</td>
<td>05 Sep 2015</td>
<td>12 Apr 2016</td>
<td>20</td>
<td>3</td>
<td>569,727.53</td>
</tr>
<tr>
<td>Single Large Credit Wire</td>
<td>1</td>
<td>06 Oct 2015</td>
<td>06 Oct 2015</td>
<td>1</td>
<td>1</td>
<td>4,699,786.00</td>
</tr>
<tr>
<td>Single Large Debit Wire</td>
<td>1</td>
<td>10 Jan 2016</td>
<td>10 Jan 2016</td>
<td>1</td>
<td>1</td>
<td>6,000,000.00</td>
</tr>
</tbody>
</table>

Table 1

In a case-based monitoring setup, a single analyst only needs to review the customer’s activities across a combination of alert scenarios, accounts and a wider timeframe (August 7, 2016 to April 12, 2016) once instead of nine individual alerts. This also ensures efficient use of AML expertise and provides a holistic understanding of the customer activities across three accounts. For simplicity, we will examine the consolidated review of the Aggregated Cash Withdrawals scenario (see Table 2):

### Aggregated Cash Withdrawals

<table>
<thead>
<tr>
<th>Alert</th>
<th>Month</th>
<th>Count</th>
<th>Amt (USD)</th>
<th>Account</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Dec 2016</td>
<td>50</td>
<td>26,354.00</td>
<td>12345678</td>
</tr>
<tr>
<td>2</td>
<td>Jan 2017</td>
<td>48</td>
<td>25,513.00</td>
<td>12345678</td>
</tr>
<tr>
<td>3</td>
<td>Feb 2017</td>
<td>29</td>
<td>29,644.00</td>
<td>12345678</td>
</tr>
</tbody>
</table>

Table 2

In the alert-based monitoring example, individual alerts might be reviewed by three separate investigators when they are generated from the monitoring system. There is clearly a lack of information to determine whether the cash withdrawals highlighted in the individual alerts are...
suspicious and the investigators would have to look back at the prior alerts as well as consider the historical cash activity of the customer to form a decision.

However, in the case-based monitoring example, the duplication of the work is significantly reduced. Only a single investigator is required to perform a three-month cash withdrawal activity review of the customer. A single investigator assigned also ensures that a consistent approach is being applied when reviewing the same customer. Holistically, the investigator will also be able to form a better understanding of the customer resulting from an extended review of the activity.

7. Conclusion

In a recent study by LexisNexis Risk Solutions - True Cost of AML Compliance APAC Survey Report, it was estimated that close to $1.5 billion per year was spent in Asia for AML compliance at banks. However, transaction monitoring analysis comprised only 9 percent of costs. The study added that “technology use at AML operations in Asia is still somewhat immature” because technology costs in Asia make up 19 percent of AML budgets compared to 81 percent for personnel costs. The study highlights the fact that there is more room for improvements in the automated transaction monitoring space in financial institutions.

Nevertheless, financial institutions need to thoroughly consider their setup by conducting risk assessments to determine which system is best suitable for the institution. A local branch office of a foreign bank may consider an alert-based monitoring system specifically tailored to the jurisdiction as the best option. However, with increasing pace of change seen in the regulatory environment, regulators of different countries may expect a direct line of communication and sharing of information within branches of a large multinational bank. As such, banks should consider moving toward adopting a case-based monitoring approach and the creation of a centralized financial intelligence unit which will be responsible in providing a consistent and holistic review of customer activities across all areas of the bank. The initial cost of investments required for the setup may be daunting, but the ultimate cost of AML failures would be spectacular in comparison.
8. Works Cited


