ORACLE
Business Process
Services

ANTI MONEY LAUNDERING

DISRUPTING STATUS QUO IN AML COMPLIANCE

With the spurt in negative news around the world on non-compliance on Anti-Money laundering, financial firms must re-think their current approach on compliance and embrace new generation technologies to bring in transformation to the current archaic process. This paper explores the current challenges faced by financial institutions and new generation technology options.

SHARANYA SAARADEEY
DEBANKUR GHOSH
RAJARSHI RAY
SRIRAM GANESAN
RAJIV RAJAGOPALAN

WHITE PAPER / MARCH 25, 2019

ORACLE

DISCLAIMER

The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle's products remains at the sole discretion of Oracle.

1.0 INTRODUCTION

Financial Crime is one of the foremost problems faced by Banks across the globe. Legislations and Regulators attention on tackling this issue became a priority after 9/11 attack in the US which led to the introduction of Patriot Act and preventing Financial Crime was introduced as the most prioritized activity for all Banks and Financial Institutions (FIs).

Economic Globalization has led to increase in Cross Border Wire Transactions, Dynamic changes in Regulatory Rules Enforcement, Introduction of Crypto-Currencies, e-commerce and web-based transactions. Money laundering and fraud transactions are growing at a fast pace and are valued at $800 Billion -$2 Trillion annually, accounting for 2-5% of global GDP (Source: UNODC survey).

To combat the evolving financial crime scenario, compliance functions are strengthened by banks all over the globe. Implementing effective KYC control [Customer Due Diligence (CDD) and Enhanced Due Diligence (EDD)] and Transaction Monitoring Rules (through various Transaction Monitoring tools and systems) are of high priority. Despite implementing many of these tools, there is an increase in compliance analysts employed to perform effective and faster investigation on alerts generated by these control tools.

Hence Banks and FIs are allocating a huge amount of their yearly budget on Maintenance and Upgrade of these compliance control systems and for alerts investigation. Any failure to ensure Regulatory compliance, Banks and FIs are fined heavily by local regulators across geographies. As of date, the world's biggest banks have been fined $321 billion and between 2009 and 2016 (Source: BCG).

2.0 CHALLENGES FACED IN COMBATING FINANCIAL CRIMES USING COMPLIANCE CONTROL SYSTEMS

Apart from the Socio-Economical and Legal aspects to the evolving Money Laundering controls, Banks also face a lot of hurdles pertaining to Data, Controls and Operation for the Compliance Control Systems in place. The below are the major hurdles faced by Banks.

1. Source Data related issues:

   Increasing data volume coupled with poor Data Quality and inadequate standardization of data structures leads to plentiful data for record keeping yet improper/insufficient data for analysis. Alongside this creating and maintaining multiple internal and external reference data sources (Internal and External Watchlists) leads to inconsistency of valid reference data.

2. Control related issues:

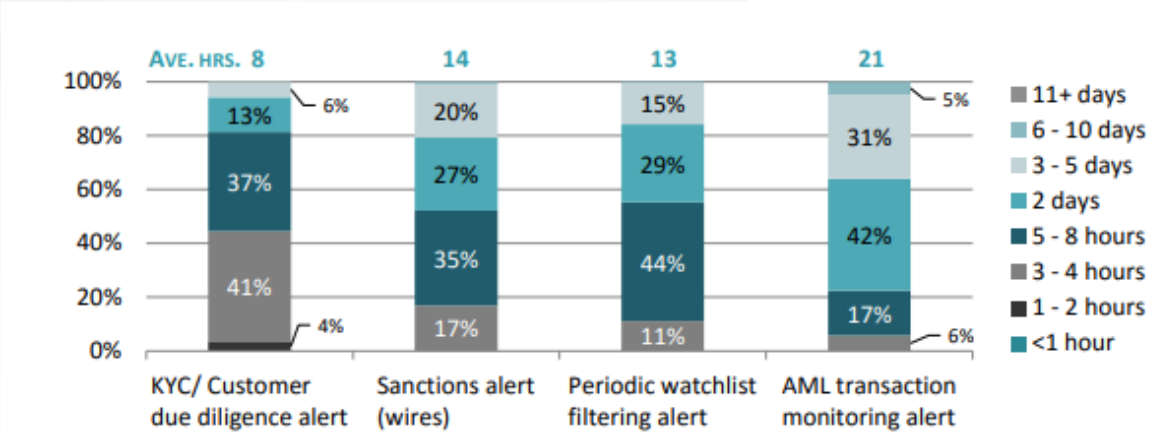
   Static rules for Transaction monitoring, Degrading controls on CDD, EDD, Sanctions Screening, Account Screening and Name screening process combined with poor Analytical approach to KYC Risk Scoring, Threshold Tuning are making the Compliance Control System become inefficient gradually.

3. Process related issues:

   Frequent change in process for SAR, CTR etc. filing, decentralized source of reference data and information for investigation causes increase in investigation time and less efficiency in the output provided.

The major staggering outcome of the above issues being generation of high volume of false positives as well as false negatives by the AML monitoring systems. As a consequence, banks have to manage ever-increasing time and effort for case investigation by compliance and operational teams. Hence Banks and FIs are forced to budget a lot of money, manpower and infrastructure, albeit without getting fruitful results.

Below diagram provides the time spent for processing alerts by major European Banks based on survey published by LexisNexis Risk Solutions. This clearly indicates it takes on more than 2 days for processing 50% of the generated alerts.



3.0 FALSE POSITIVE

A false positive is an error in AML and compliance monitoring process, in which a scenario or condition tested for is mistakenly found to have been detected. At the current AML and compliance setup in a typical firm, this “error” could only be spotted after utilizing a handful of manual and computational resources on a regular basis.

To find out what a false positive is, let us consider an example, where a service holder performs regular transaction of $1000 every month to a specific savings account. Based on the customers KYC and regular transaction pattern it is observed that this transaction activity is as per normal behavior. Due to a sudden spike in the income of the customer an alert is generated as the threshold amount is breached. After investigation it was found that the customer sold one of his properties and gained a fund of $60,000 in his account. As this transaction has a legitimate source and the behavior is not suspicious, this alert can be considered as a False Positive (False Alert) match and can be closed.

Among all the alerts being raised daily, around 90-95% of them are False Positives. False positives add to huge percentage of resource utilization from Operational perspective. This results in substantial amount of cost for the investigation efforts, and consequently, this becomes a prominent contributor to the overall annual cost that firms need to consider for running their AML and Compliance operations.

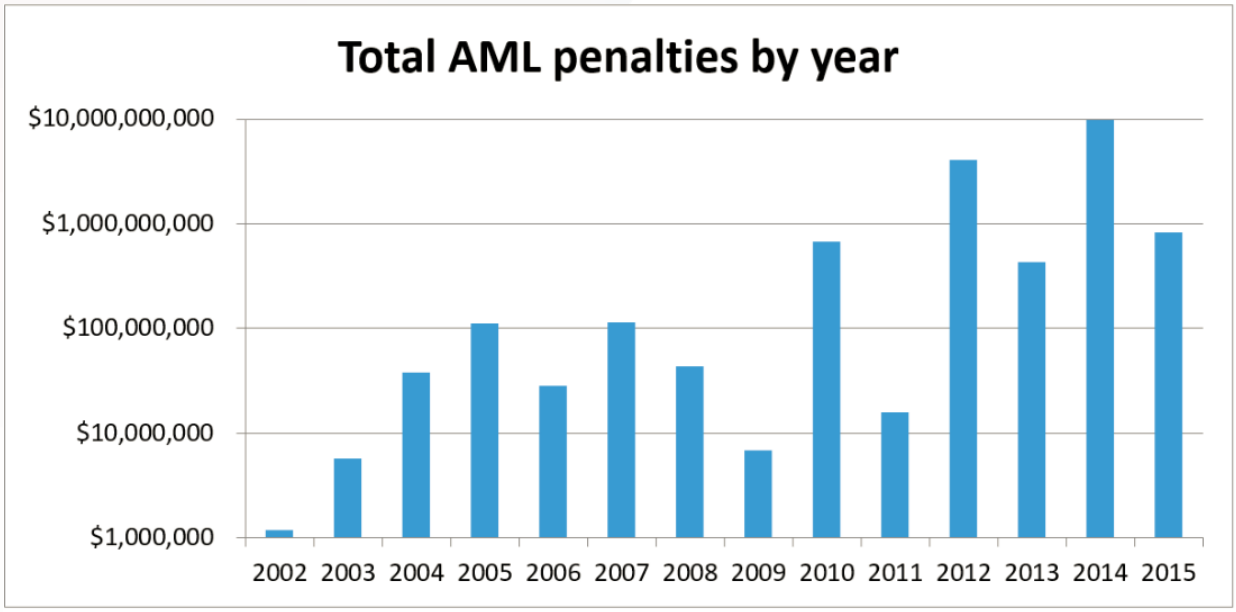
4.0 FALSE NEGATIVE

False negatives are exactly the opposite of false positives. These are genuine alerts that banks and FIs have missed to detect and allowed to go through their systems.

A classic example of a false negative is where students’ accounts are being used as “Money Mule” Accounts. Let us first understand what is meant by Money Mules. A money mule / ‘Smurfer’ is an individual who transfers money acquired illegally on behalf of others. Typically, the mule is either paid for services or sometimes they are unaware of the fact that they are being used for money laundering. Students being used as “Smurfs/Money Mules” are very common as they are hard to detect in the law enforcement radar. The reason being, their profiles mostly are low risk and the transactional activities appear to be usual pertaining to daily expenses.

To quote another example, a student from a high-risk country studying abroad receives nominal funds from source country with purpose of daily/educational expenses. This money is either utilized or withdrawn. Though the transaction has got originated from a high-risk country, the alert will not get generated in this case because risk associated with the beneficiary is low and the activity appears to be usual. With evolving rules and pattern matching at the granular levels, these types of false negatives can be detected and converted to true matches.

Such incidents can cost the bank a fortune and loss of reputation because of non-adherence to Regulatory Compliance. Below graph (Source: Accuity) depicts banks have been paying penalties excess of $100MM from 2012.



Source: US Department of Treasury, Office of Foreign Assets Control

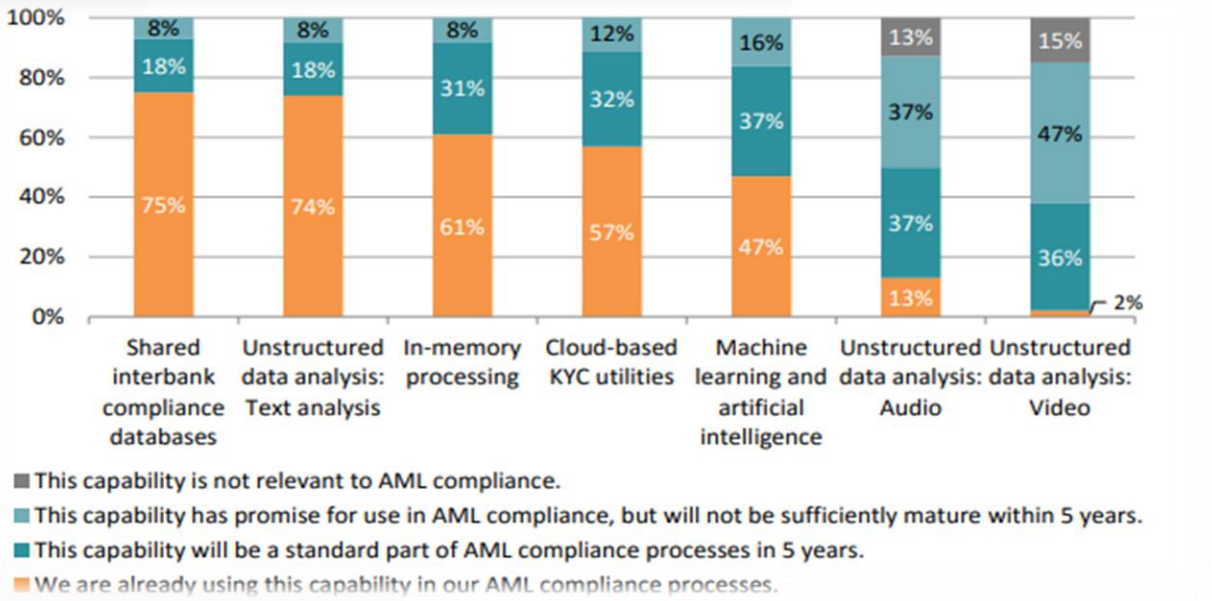
5.0 POSSIBLE SOLUTIONS TO IMPLEMENT AN EFFICIENT REGULATORY MONITORING SYSTEM

Now let us look at the various options that Banks and FIs can look at for an improved and efficient regulatory monitoring system. Optimizing and enhancing the existing transaction monitoring system is one of the options. Corelating multiple related alerts, auto-closing alerts based on rules defined in the system could certainly minimize the numbers of alerts for investigation. However, this could be productive up to a certain threshold. For a long-term solution, newer technologies like Machine Learning (ML) and Robotic Process Automation (RPA) could be of great assist to Banks and FIs in this situation.

These new technologies will help Banks and FIs simultaneously optimize infrastructural costs as well as improve users' efficiency. At the same time, this would help Banks and FIs shift their financial-crime and compliance activities toward a more forward-looking and sustainable approach.

6.0 BANKS AND FIS: EMBRACING NEW TECHNOLOGIES

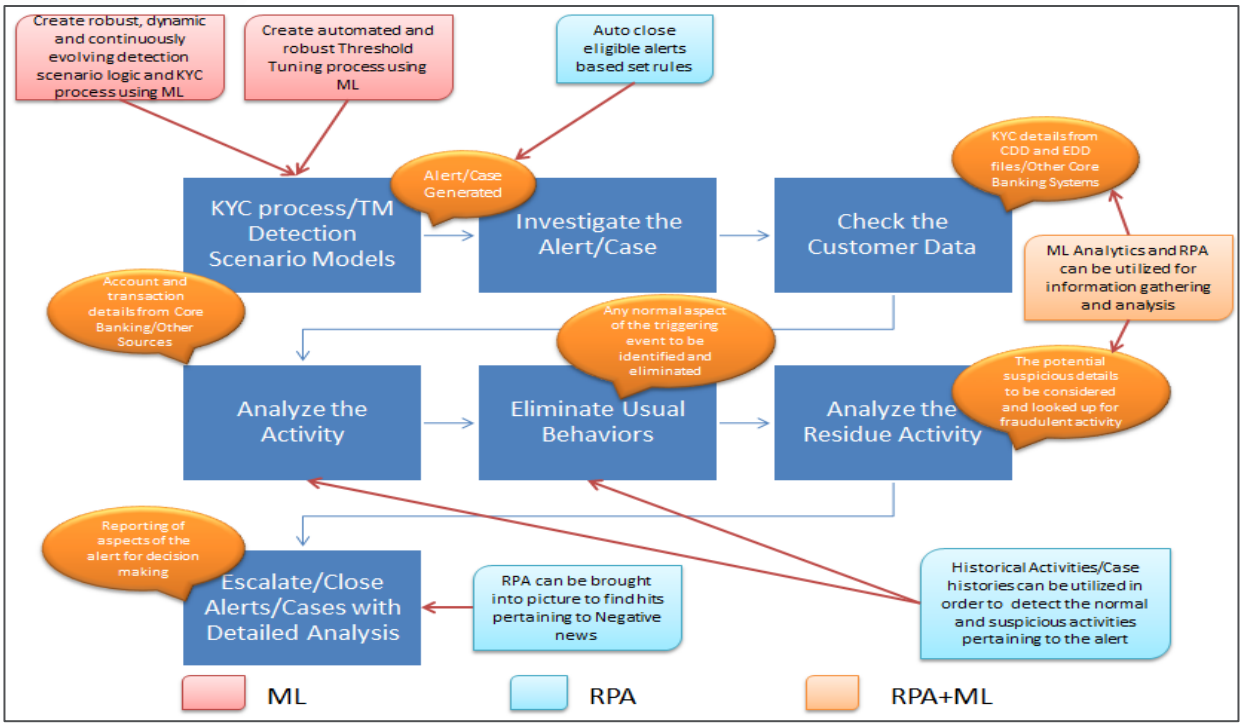
To respond to the current needs for combating money laundering threats and to circumvent growing challenges faced during alert and case management procedures, Banks have started looking at new technologies for AML Compliance.



**Source: 2017 True cost of AML compliance LexisNexis Risk Solutions*

7.0 DISRUPTING AML PROCESS THROUGH TECHNOLOGY INNOVATION

This section will provide an insight on how the new technologies are useful in bringing efficiencies in case resolution and regulatory filing in AML and compliance areas in Banks and FIs. The below diagram depicts where possible solutions can be introduced into the AML workflow.



Machine learning in creating Robust and Dynamic behavior detection model:

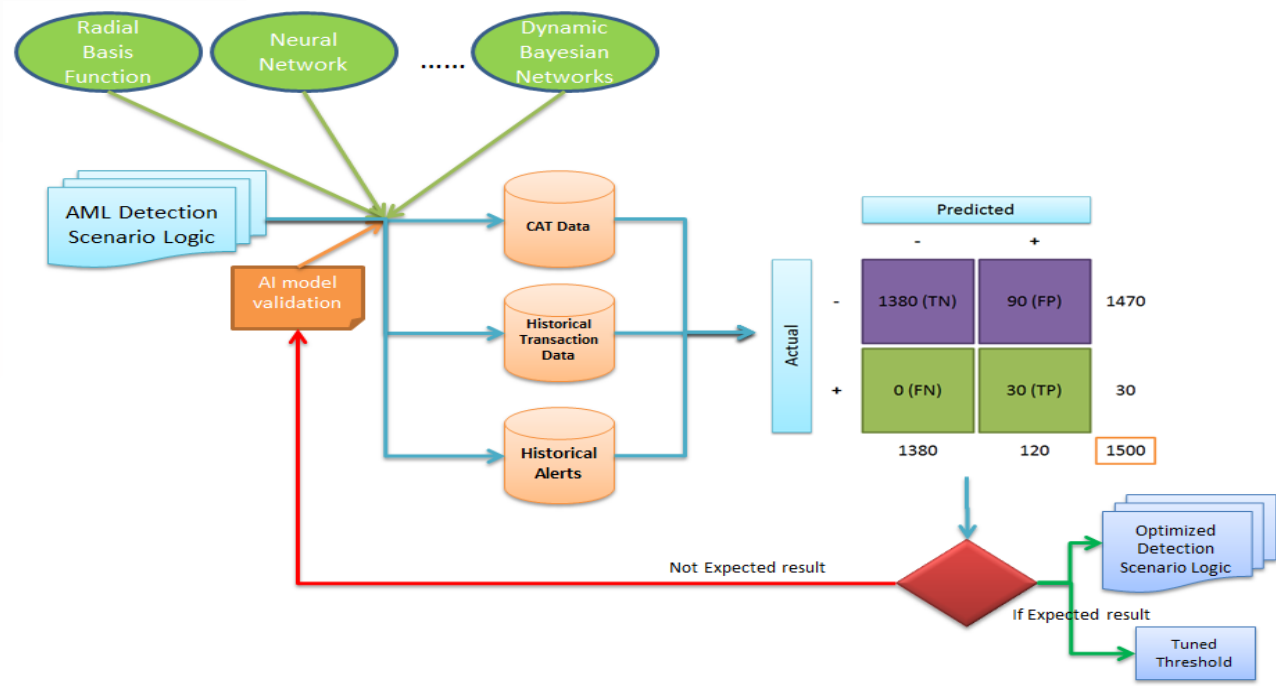
Machine Learning algorithms can be used to select the best algorithms for making better predictions from a dataset. Machine Learning models can bring in more parameterized values, discover hidden links and relate usual behavior to create an optimized model for restructuring the existing behavior detection scenario logic. Latest research reveals how techniques such as Radial Basis Function, Neural Networks and Dynamic Bayesian Networks have been successful at classifying Money Laundering transactions with greater accuracy.

Machine learning in KYC/CDD process:

With banks focusing their resources on increasing the quality of data for monitoring, they can also bring in advanced statistical algorithms to risk score customers and accounts. With less paperwork involved in collecting KYC data, machine learning can collect more information about the customer at regular basis and from adverse sources (like prompting to take selfies from mobile devices to geotag the customer, or gathering information from social media profiles to understand personal behaviors and inter-personal links of the customer etc.)

Machine learning in creating dynamic threshold tuning process:

Datasets can be carefully constructed to avail present and historical data (including Customer, Account, Transactions and historical Alerts). A machine learning platform can look at historical data sets on alerts and corresponding investigation outcomes. Based on this information, it will determine the best ways to pre-process the data, structure it for validation and final holdout assessment, distill out the relevant features related to money laundering and identify the best machine learning algorithms to apply based on this dataset. Bank could then select the model they think is most robust and efficient by its performance on the validation data. They can observe the score threshold below which no SARs would have been present (i.e., the threshold yielding zero False Negatives, or FN). The True Negatives are cases that investigators would have been correct not to review, and thus it represents the efficiency gain. All the True Positives, the actual SARs, would have been captured above the threshold. Consequently, the resulting new False Positive rate is reduced relative to reviewing all the cases.



**Source: Diagram created based on information from article "Enhancing an Anti-Money Laundering (AML) program using Automated Machine Learning" published in blog.datarobot.com. (TN: True Negative | FP: False Positive | FN: False Negative | TP: True Positive)*

Once the analyst verifies the threshold on the holdout sample (which is the random sample not used to train or validate the model, including selecting the score threshold), the model is ready for production.

Machine learning in Auto-Closure of Alerts/Cases:

Alerts auto closure can be achieved by applying appropriate weightage to the various Customer related parameters (List: See below) in a learning algorithm.

1. KYC Risk
2. Country of Residence Risk
3. Industry/Occupation risk
4. Customer Type (Individual, Trust etc.)
5. Watch List hits
6. Number of Accounts
7. Number of escalated cases in the last year
8. Number of SARs etc.

The learning algorithm uses this information and computes the Alert / Case Risk. Separately the customer risk is calculated using the Customer information applying the desired weightage. The risk level of both the Customer and the Alert / Case risk from the learning algorithm can be plotted into a 2X2 matrix and used to determine auto closure of a generated alert as well as routing to appropriate seniority group for better investigation

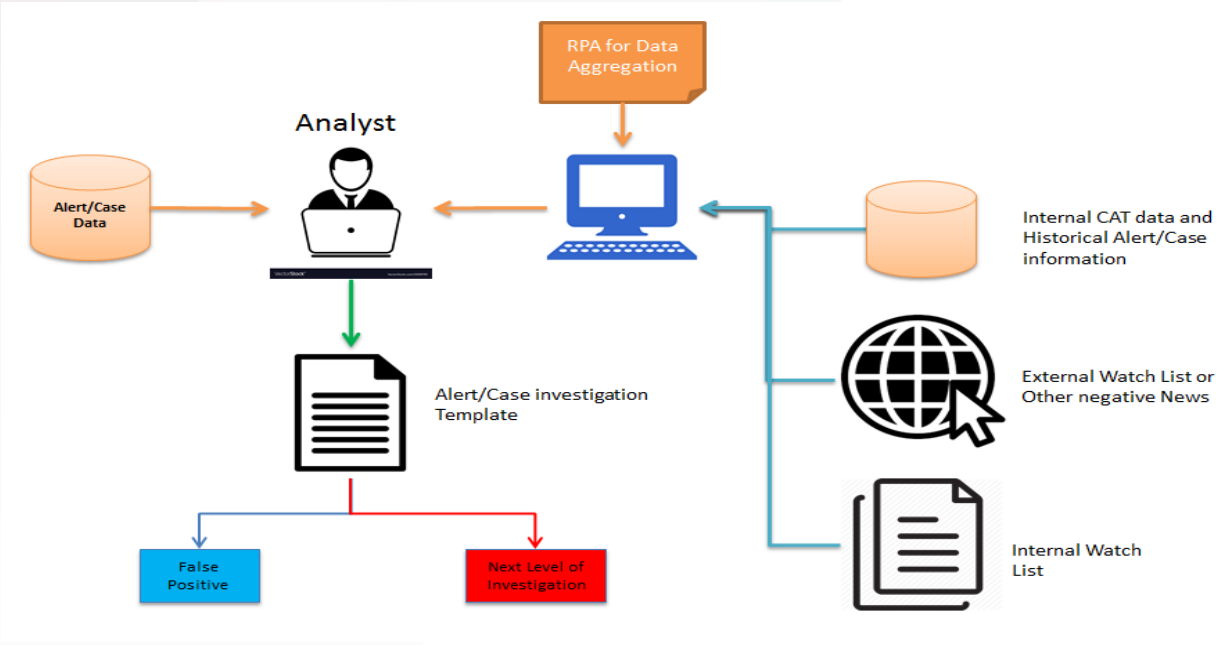
Predicted Alert / Case Risk	Customer Risk	Rule based Decision framework
Low	Low	Close
Low	Medium	Group 1
Low	High	Group 2
Medium	Low	Group 1
Medium	Medium	Group 3
Medium	High	Group 2
High	Low	Group 2
High	Medium	Group 2
High	High	Group 3

Group 1: Lower level Group 2: SME's Group 3: Medium level

Alerts/Case can also be closed by creating an algorithm to parse the alerts/cases into homogeneous risk buckets based on primary evaluation. After evaluation, when investigator closes one alert in the given bucket will result in closing all related alerts/case in the same bucket.

Data aggregation for Alert/Case Investigation:

As of today, an analyst requires anywhere around 30-45 minutes on an average to investigate an Alert/Case (Source: Transforming AML Compliance with RPA - TCS). The major part of the time is invested in gathering information regarding the Customer, Account and Transactions from various external and internal sources. RPA can be introduced to fetch relevant structured/unstructured data into a single user-friendly format, correlate data from multiple sources (including historical Alerts and CAT (Customer, Account and Transaction) Data and help fill up standardized investigation template with required information. More the use of standardized template with adequate data, less time for is required for investigation. With RPA involved, Alert Investigation time can reduce up to 70% (Source: Transforming AML Compliance with RPA - TCS).



8.0 CONCLUSION

Machine Learning and RPA have great potential in bringing efficiencies in the investigation process and help optimize time and effort for the same. Futuristic solutions can be implemented for effective data integration, reduction of false positives and conversion of False negatives to True Matches in the Monitoring system. These new technologies can certainly help Banks and FIs to build a whole new financial system with better security against Money Laundering and Financial Fraud coupled with higher accuracy and effectiveness.

Reference

Following are the sources of information for the documentation above:

- Oracle AML SMEs
- Articles by ACAMS Today
- Surveys by LexisNexis Risk Solutions*: https://risk.lexisnexis.com/global/-/media/files/corporations-and-non-profits/research/true-cost-of-aml-compliance-europe-survey-report-pdf.pdf*
- Survey by US Department of Treasury and OFAC and posted by Accuity: *https://accuity.com/press-room/accuity-research-shows-25-drop-global-correspondent-banking-relationships-linked-de-risking/aml_penalties_by_year/*
- *Survey by UNODC: https://www.unodc.org/unodc/en/money-laundering/globalization.html*
- Survey by Boston Consulting Group (BCG)
- Blog in Datarobot.com on Anti-Money Laundering program using Automated Machine Learning: *https://blog.datarobot.com/anti-money-laundering-using-automated-machine-learning*
- Blog in L&T Infotech site on Machine Learning to reduce false positive in AML: *https://www.lntinfotech.com/blogs/using-machine-learning-to-reduce-false-positive-in-anti-money-laundering-aml/*
- Blog in TCS site on Transforming AML Compliance with RPA: *https://www.tcs.com/blogs/transforming-aml-compliance-with-rpa*

ORACLE CORPORATION

Worldwide Headquarters
500 Oracle Parkway, Redwood Shores, CA 94065 USA

Worldwide Inquiries
TELE + 1.650.506.7000 + 1.800.ORACLE1
FAX + 1.650.506.7200
oracle.com

CONNECT WITH US

Call +1.800.ORACLE1 or visit oracle.com. Outside North America, find your local office at oracle.com/contact.

blogs.oracle.com/oracle facebook.com/oracle twitter.com/oracle

Integrated Cloud Applications & Platform Services

White Paper Title
January 2017
Author: [OPTIONAL]
Contributing Authors: [OPTIONAL]

Oracle is committed to developing practices and products that help protect the environment

ORACLE