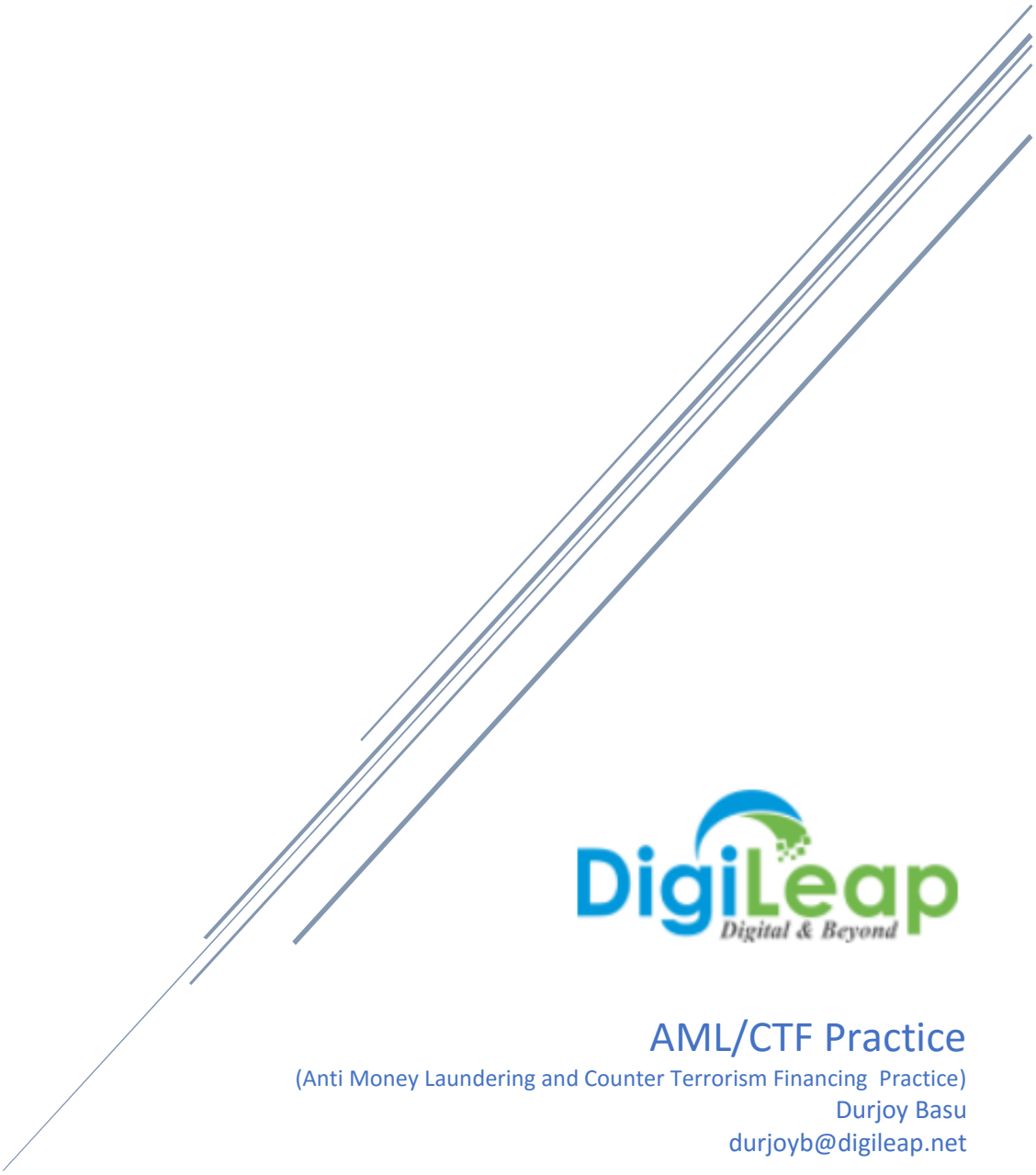
TRANSACTION MONITORING CAPABILITIES

Digileap Whitepaper



DigiLeap
Digital & Beyond

AML/CTF Practice

(Anti Money Laundering and Counter Terrorism Financing Practice)

Durjoy Basu
durjoyb@digileap.net

Contents

Capabilities of Transaction Monitoring systems

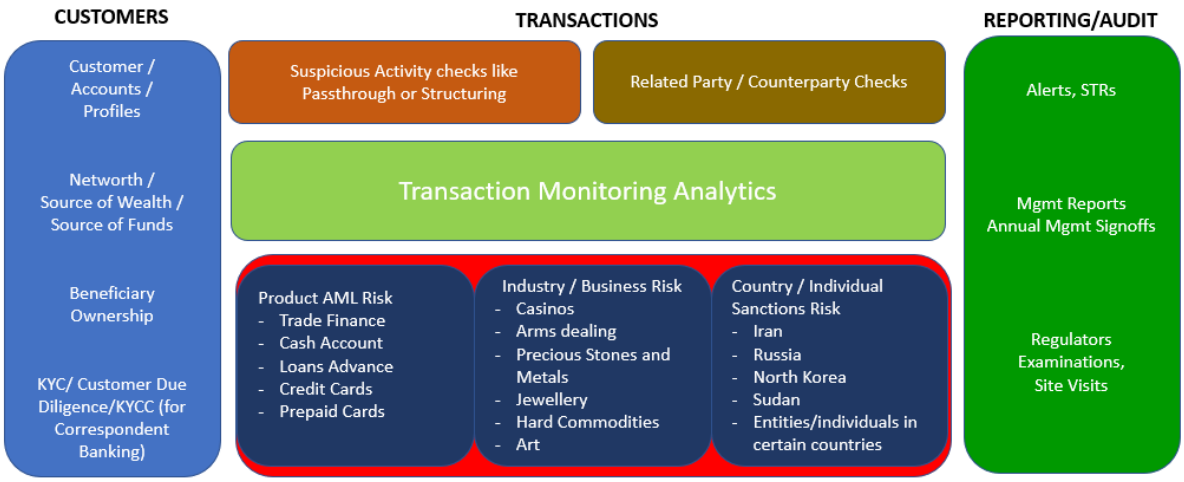
The capabilities of transaction monitoring systems should be commensurate with the financial institution's (FI's) risk profile with that involves its mix of products, services, customers, entities and jurisdictions that it serves. The FI's risk in its different lines of business (Retail, Private, Corporate and Investment Banks) may vary depending on each vertical's appetite for risk.

An effective transaction-monitoring process and system should have the ability to:

- Analyse the client's account/transaction history with the client's specific profile information and relevant profile group
- Compare transaction history to risk scoring models to identify patterns of suspicious activity or anomalies.
- Track the alerts to manage them and report those that signal suspicious activity.
- Maintain an audit trail for future reviews and provide aggregated statistics

The limitations of TM systems are however exposed when rules set up either:

- Do not capture a major portion of the cases that should have been flagged as suspicious transactions
- Flag an excessive number of false positives leading to a huge increase in investigation staff
- Do not reflect changes in regulation or products, services, geography added or discarded
- Or do not reflect changes in customer risk profile quickly enough or linkages to other accounts/customers who may be involved in suspicious transactions.



Risk Based Approach in TM Systems

The key to improving reliability of TM systems is to take a Risk Based Approach (RBA) depending on the Products, Services and Geographies that a bank operates in. A few ways to do that are:

- Segment out low-risk population group and apply higher thresholds, thus generating fewer alerts for them. Customer type (large corporation, mid-market company, sole proprietor) is important

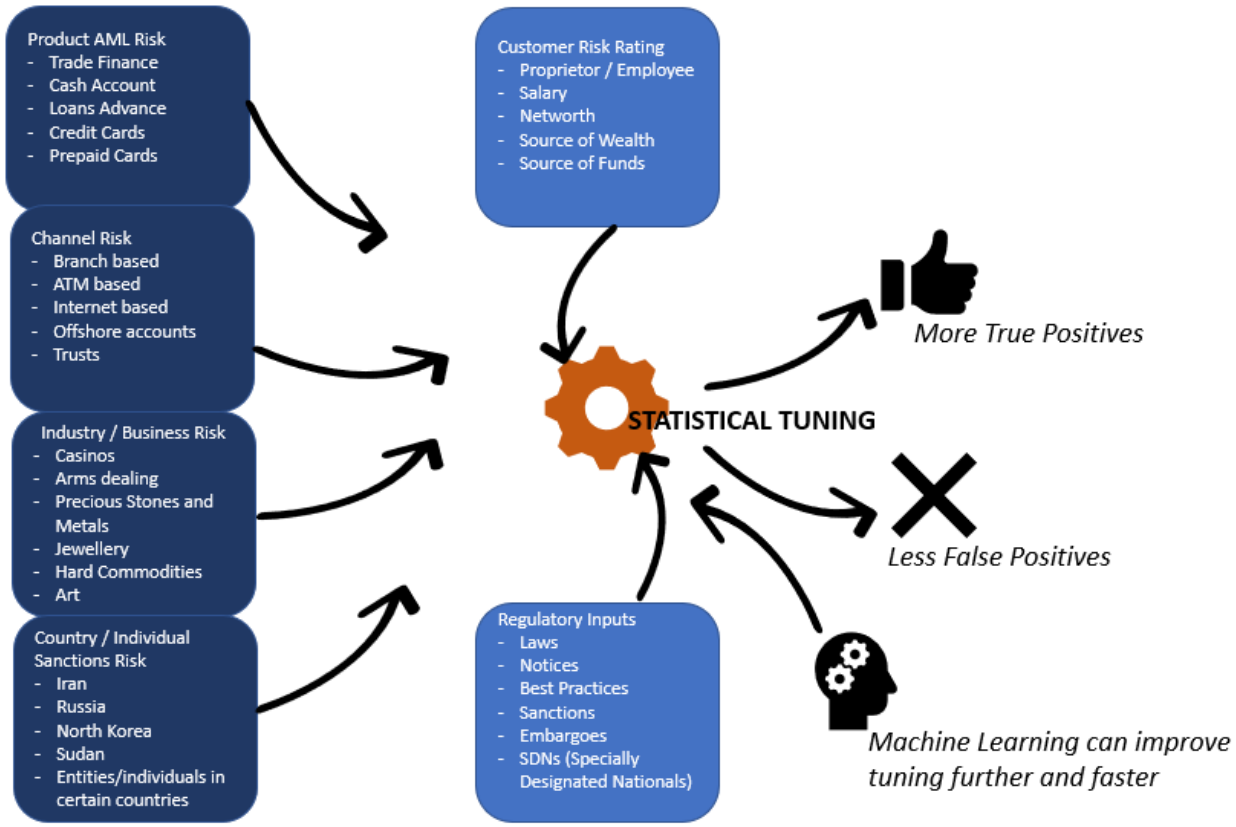
- Focus your effort on higher risk products, channels, services and geographies with a lower threshold for alerts.
- Make sure that for each product, service or channel you have different rules to cover multiple types of risks
- Suppress alerts which have previously repeatedly (say three times) turned false and turn them on only for re-check after certain number of suppressions (say ten times).
- Keep adding different typologies/attributes and more alert thresholds to micro-segment your entire customer base into different profile groups. Micro segmenting helps as the bank can get more granular about the risk.
- Establish a group that constantly audits the TM system against new regulations and products. And tests segments and thresholds for validity. Eliminates overlapping rules and those no longer in use.

Statistical Tuning

In situations where the number of conversions from alerts to (positive) cases is high, the institution is doing a better job in managing its false positives. The goal therefore should be to lower false positives through statistically tuning the scenarios and finding those typology/threshold combinations that repeated provide a good match for suspicious transactions.

There are three key challenges in managing false positives:

- Poor segmentation or typology selection. Typologies here relate to attributes like customer-type, products, services, geography, profile groups, counterparties, transportation vehicles, documents, watch lists or sanction lists
- Creating proper rules (also called scenarios) using the typologies so that they are relevant in identifying transactions that signify abnormal behaviour.
- Identifying the appropriate threshold values to tweak the rules to be relevant



Segmentation Challenges

There are multiple challenges in segmenting the customer base, namely:

Poor Quality Customer data

The data collected at onboarding and during periodic Client Due Diligence (CDD) reviews may be either incomplete, plain wrong or out-of-date. Trying to segment the customer base on erroneous or unavailable information like customer occupation, industry, counterparties, transaction ticket size, transaction frequency, means segmenting customers into proper profile groups will simply not happen.

No centralized database

In order to collect information regarding customers and accounts from multiple lines-of-business and multiple banking-product transactions running on different systems, a centralized database or data-warehouse is required. Without this, an all-round customer profile cannot be generated, let alone assigning the profile to the appropriate profile group to track good or bad behaviour.

Scenarios based on very few typologies or attributes

The customer base has to segmented out using a combination of different typologies including customer information, product or service information, transaction channels, geographies with risks associated with each typology.

Need for a phased iterative approach to segment identification

Once the typologies have been identified, a thorough analysis needs to be done on the data to set proper thresholds. The data should not be polarized into lumpy segments. This is an iterative process of re-segmenting by changing thresholds for each attribute so that the spread of data is proper.

Need to periodically retune scenarios and thresholds

Due to regulatory updates, additional sanctions, product and services changes, newer channels, there may be a need to modify, add or delete scenarios. Thresholds may need to be changed for existing scenarios to reflect risk level changes. All this requires periodic retuning. The frequency depends on the bank's coverage of products, services, geographies and the rate of changes.

Larger institutions would need more frequent changes leading to almost a continuous effort at retuning. Also, a rapid increase in customer base, particularly addition to products or geographies, may lead to polarized segments that would need to be re-segmentized by adjusting thresholds of attributes. A documented retuning process is a must and usually asked for by Regulators during site visits with evidences of following the process.

Conclusion

As can be seen from the challenges and opportunities outlined above, setting up transaction monitoring systems is a fairly elaborate process, requiring cooperation and coordination of different lines of business (LOB), AML Operations, Compliance, Technology and TM vendor experts.
It requires customer, product and services data to be centrally available and validated for quality. Setup of scenarios based of appropriate typologies and thresholds tuning is no simple effort. AML Operations also has to be engaged in continuously retuning scenarios to reflect the changing situation on the ground.

There is no escaping TM systems implementation as they have become mandatory as far as regulators are concerned. All this leads to the establishment of a Program Lifecycle arrangement which we will discuss in the next article.

Write to us at info@digileap.net or durjoyb@digileap.net to know more about Transaction Monitoring or our services.