Deloitte.

Transaction Monitoring Optimisation

Using an intelligence lead approach to Transaction Monitoring

Contents

Introduction

Transaction Monitoring (TM) is "the process of monitoring transactions after their execution in order to identify individual unusual transactions, including monitoring single transactions as well as transaction flows".[1] The Central Bank of the United Arab Emirates (CBUAE) similar to other central banks / regulators require all Financial Institutions (FI) to establish and maintain effective transaction monitoring and sanctions screening programmes consisting of calibrated risk-based frameworks, training and awareness of their employees, with active oversight by the board. Furthermore, regulators require FIs to ensure the ongoing enhancement of their transaction monitoring and sanctions screening systems based on their risks, and subject their monitoring and screening models to independent testing, validation and auditing.

Most FIs have a TM system, configured with rules and scenarios based on Anti-Money Laundering (AML)/ Combatting the Financing of Terrorism (CFT) typologies, which analyse the details of all transactions processed by the FI. The TM system flags a transaction as suspicious if it meets the criteria of the rules/scenarios configured and generates an alert. These alerts are then analysed/adjudicated by the FI to determine whether the transaction needs to be escalated for further investigation and potential filing of a suspicious activity/transaction report (SAR/STR) with the Financial Intelligence Unit (FIU).

Why is Transaction Monitoring important?

In today's interconnected financial system, TM has become a fundamental element of a FI control framework. TM is vital in the ongoing fight against financial crime by identifying and stopping the flow of illicit transactions. The United Nations Office on Drugs and Crime (UNODC) estimates the amount of money laundered globally per year to be approximately 2% - 5% of global Gross Domestic Profit (GDP), or USD800bn – USD 2tn[2], which highlights the growing need for FIs to implement a robust TM program.

Below are some key reasons for FIs to have an effective TM framework in place:

01. **To remain compliant and avoid regulatory breaches**
Regulators mandate FIs to monitor transactions and alert on suspicious activity, and are clamping down on FIs that are in breach of this requirement. Regulatory compliance firm Fenergo estimates FIs to have paid over USD 10bn in financial crime related non-compliance fines in 2020 alone.[3]

02. **To spot financial crimes before they take place**
Bribery and corruption have a direct link to poverty as it delays and distorts economic growth. They thrive upon weaknesses in institutions and are facilitated by money laundering. An effective TM program can help an FI prevent illicit transactions and activities that impact individuals' lives, communities and the wider economy.

03. **To aid the adoption of a risk-based approach**
By monitoring transactions on an ongoing basis, FIs can better understand their customers' risk profile and patterns of activity, allowing them to direct their monitoring resources more efficiently. TM outcomes are also increasingly being considered as input into more dynamic Customer Risk Assessment (CRA) methodologies which aim to use a behavioural risk approach to assessing a customer's AML/CFT risk.

04. **To better understand and service customers**
An effective TM program can help FIs better understand their customers' transaction patterns, allowing them to provide input into product/service development and marketing functions, and to tailor service offerings and increase their share of the wallet.

Regulatory reforms in the Transaction Monitoring landscape

Financial services remain one of the most highly regulated industries, and regulators around the world are increasingly focusing their emphasis on TM regulatory frameworks.

UAE Central Bank (CBUAE)
In June 2021, CBUAE issued guidelines requiring FIs to file Suspicious Activity Reports (SARs) within 35 days.

Monetary Authority of Singapore (MAS)
In 2018, MAS released a guidance paper outlining its supervisory expectations with respect to licensed FI TM programs.

Financial Intelligence Centre (FIC)
In 2019, South Africa's FIC issued guidelines mandating SARs to be filed within 15 days of an FI becoming aware of potentially suspicious activity.

1. Wolfsberg Statement: Monitoring Screening and Searching
2. United Nations Office on Drugs and Crime: Money Laundering
3. Fenergo: Global Financial Institution Fines for AML, Data Privacy and MiFID Rise 27% in 2020

Challenges in the existing Transaction Monitoring landscape

While there is a marked shift in thinking towards more advanced TM capabilities using Artificial Intelligence (AI) and Machine Learning (ML), most FIs still use a traditional, rules-based TM system, which limits their ability to keep up with the sophistication of the criminal activity. Furthermore, FIs have been operational for decades and over time have connected different systems and processes with the introduction of new services and offerings. Therefore, there are often disparate sources of data across the FIs which leads to inconsistent and poor-quality data.

Below are a few of the challenges faced by FIs impacting TM:

01. Traditional technology and systems
    The data collected by these systems is often limited, the rules/scenarios can reduce their ability to be configured and rely on static data and data collection. Processing can be complex and cumbersome due to archaic data modelling and storage methodologies and technologies.

02. Poor data quality
    Data quality is a cornerstone of an effective TM system – FIs must rely on the accuracy, consistency and completeness of data, without which potentially illicit transactions can go under the radar and remain undetected. An example of poor data quality is the incorrect tagging of customers to different business segments e.g. retail customers being tagged as SME customers and vice versa. Poor data quality leads to an inability to rely on the automated alert generation process. This results in a significant increase in operational effort and cost due to the manual activity required to give integrity to the results generated by the system.

03. False positives
    Due to the poor quality of data being fed into the TM systems, coupled with the limitation of dynamic monitoring, FIs are increasingly faced with large volumes of alerts being generated. In this instance it is required for FIs to have large teams of resources to review and analyse alerts which increases the operational risk and cost of compliance, with little to no effect on the primary objective, i.e. the fight against financial crime. Even with a large pool of people reviewing alerts, most (if not all) FIs still have significant alert backlogs, which again defeats the purpose of TM. What good is there in identifying illicit activity weeks (if not months) after it has taken place?

04. Regulatory consequences
    In an attempt to keep pace with the number of alerts being generated and to clear the alert backlogs, many FIs have been compromising on the quality of investigation completed prior to closing an alert. There have been instances where alerts have been closed without the necessary justification and/or without any supporting documentation to evidence the conclusion. Alternatively, FIs have started to file defensive SARs/STRs. This is not looked at favourably by the regulators, as the focus should be on fighting financial crime, rather than just maintaining compliance. Regulators also expect FIs to conduct periodic typologies assessments and to consider updates to their existing TM scenarios/rules in line with changing ML/FT trends as identified by Financial Action Task Force (FATF), FINCEN etc.

Recent TM optimisation regulatory guidance

In June 2021, CBUAE issued guidance for Licensed Financial Institutions (LFIs) on TM optimisation and suspicious transaction reporting.[4] The guidance, designed to provide LFIs with a framework to help them comply with CBUAE AML laws and regulations, touches upon the following aspects of optimising their existing TM systems:

- Rule definition and pre-implementation testing: LFIs should employ TM detection rules/scenarios that are designed to identify suspicious patterns and elevate them for review. This can be achieved by performing risk-based customer and product segmentation, employing statistical tools to fine tune calibrations and performing pre-implementation testing of TM rules to ensure compatibility.

- Alert scoring and prioritisation: LFIs should consider assigning risk-weighted scores to prioritise higher risk alerts for an expedited review.

- Post implementation testing, tuning and validation: LFIs should reassess the functionality of TM systems and processes, including the continued relevancy of detection scenarios, assumptions and calibration of rule threshold values and parameters.

- LFIs are ultimately responsible (…) to report suspicious activity without delay and should seek to file STRs and SARs (…) within 35 days from alert generation. As a result, the CBUAE considers defensive STRs or SARs as indicative of an inefficient transaction monitoring system and an LFI's weak system of internal controls.

- LFIs should test and validate the integrity, accuracy and quality of data to ensure that accurate and complete data is flowing into their TM program. Data testing and validation should typically occur atleast every 12 to 18 months.

4. Central Bank of the United Arab Emirates: Guidance for Licensed Financial Institutions on Transaction Monitoring and Sanctions Screening, September 2021

Next steps for Transaction Monitoring

FIs process thousands of transactions per day, each carrying a vast array of information which can help the FI form a clearer picture of its customers. Through a combination of leveraging this information and embarking on a journey to enhance their TM systems, FIs can better understand who they are transacting with.

Given the various challenges associated with legacy TM systems, FIs can benefit from a combination of undergoing a TM optimisation process and harnessing a multitude of technological developments to seamlessly combat the contemporary and evolving risks of being used as vehicles for illicit transactions.

Benefits of the optimisation process
Embarking on a journey to optimise their TM systems requires FIs to deploy a smarter and more data-driven approach. Not only can this process help overcome the common challenges being associated with legacy TM systems but can also derive numerous benefits to the FI:

01. Enhanced efficiency
    Optimised TM systems can increase the effectiveness of identifying suspicious activity and allow for greater focus to be placed on areas where the risk lies. Harnessing technologies allow for dynamic data to be considered that will help FIs finetune their TM rules, scenarios and thresholds, thereby reducing the volume of false positives generated while ensuring true negatives are not missed. This can have the trickle-down effect of helping

FIs increase the overall efficiency with respect to speed of high-risk case escalation and quality of SAR/STR submission. These being particularly pertinent in an age wherein regulators are increasingly looking for FIs to expedite the rate at which they detect illicit activities.

02. Optimal client segmentation
    Client segmentation is a key component of a Risk-Based Approach (RBA) at its simplest, an RBA means identifying the areas that present the greatest financial crime risk and allocating sufficient resources to mitigate them accordingly. By harnessing dynamic data driven insights, optimised TM systems can better consider the transactional (and other) behaviour of clients and account for this behaviour, allowing FIs to cluster customers and set more precise TM parameters and thresholds for those with similar behavioural patterns.

03. Cost reduction
    One of the most prevalent challenges associated with legacy TM systems is the sheer volume of false positive alerts generated, each requiring costly and time-consuming manual reviews. By optimising TM systems, FIs can categorise and prioritise alerts, and make decisions on a more intelligent and risk-based approach, leading to potential auto/semi-auto closure of alerts. This approach does not only automate the first level of reviews, but can also provide more intelligence and context to investigations teams dealing with higher

risk alerts and therefore create better efficiency in these processes to overall reduce compliance costs and focus resources on high-impact activities.

04. Improved oversight
    Coupled with the ability to process and analyse larger sets of data in a quicker and more accurate manner, FIs can meet the stringent regulatory reporting timelines. Furthermore, management information and data analytics can identify links, relationships, patterns and behaviour to generate detailed insights that can inform governance oversight through interactive monitoring dashboards.

Transaction Monitoring optimisation journey
Amidst the various opportunities and benefits to optimising TM systems, there are several mechanisms available to FIs through which they can embark on this journey – these include improving their existing systems, introducing new technologies such as Artificial Intelligence (AI), Machine Learning (ML) and Intelligent Automation (IA) into the TM process. Applying methods to establish a more targeted approach to transaction monitoring that combines financial crime and analytics expertise can enable FIs to modernise their TM systems and allay the challenges associated with maintaining legacy systems.

It is essential for FIs to have a clear understanding of the approach best suited and compatible with their organisation, systems and structure.

Improving existing Transaction Monitoring systems

One way to address the deficiencies of a TM framework and improve the efficiency of the TM process, is to look at the existing systems, fine-tune the thresholds used to generate alerts, review the typologies and the linked scenarios, add scenarios which are not available and to use a RBA to remove redundant scenarios.

The following are the steps required to review the existing TM framework:

01. Desktop analysis and typology research
   TM scenarios typically fall under two categories: those that respond to a specific risk or typology and those that identify suspicious behaviours or patterns. Analysing existing TM rules through desktop analysis can help the FI identify gaps in its TM framework.

For example:
A. A rule that generates a large volume of alerts may indicate that the rule is ineffective in its current form and may therefore require finetuning.
B. On the other hand, a rule which has a high percentage of conversion into SARs may indicate that it is working effectively and achieving its goal of identifying potentially illicit transactions.

Analysing known typologies can help FIs identify a scope for new TM rules. Examples of typologies identified by leading international best practices include:

Best practice	Thematic consideration		Typology
ACAMS	Commercial viability		Unwarranted and unexplained transfers
	Circulation of funds		Repeat import/export of high-value commodities
FATF	Layering of funds		Over or under-valuation of property
	Layering of funds		Complex loans and credit finance

02. Data led analysis
   Analysing alert data can provide insights into the effectiveness of FI's existing transactions and TM rules, and provide a basis for recommending optimisation. This analysis can involve a multiple step process:
   A. Assess the number of alerts to determine the frequency with which a particular rule is flagged.
   B. Conduct bucket analysis to sort the frequency with which a rule is flagged across various parameters e.g. by transaction value, account type, client risk rating etc.
   C. Determine scope for finetuning the rules based on the analysis conducted, using various metrics such as alert-to-SAR conversion rate, volume of false positives etc.

Leveraging analytics can also help FIs proactively identify risks and opportunities across a range of preventative financial crime use cases, helping to reduce operational workloads in case management. FIs may also be able to implement more targeted transaction thresholds by leveraging the historical information gathered through data analysis.

03. Simulation
   Simulation-led data analysis can provide insights into threshold tuning for optimisation of TM rules and allow the FI to identify the effects of changing thresholds without having to implement them. Experimentation in a sandbox environment can help the FI improve the flexibility and adaptability of rules for TM, providing a testing area to build new rules or change existing ones.
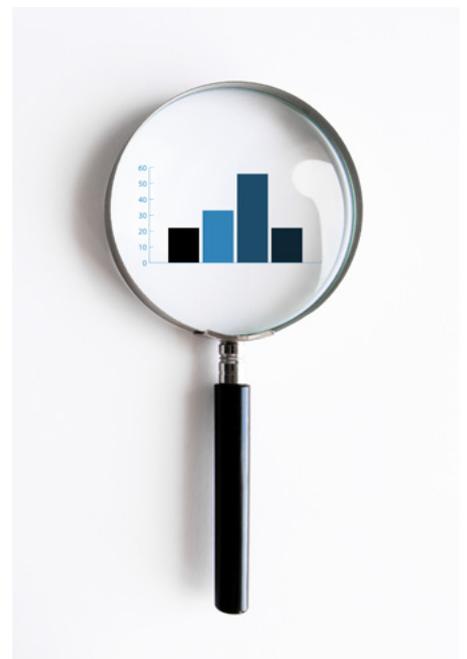
Introducing new technologies into the Transaction Monitoring process

The second option available to FIs to achieve TM optimisation is to introduce new technologies such as AI. There is a growing consensus that adopting technological innovations including robotics, cognitive automation, machine learning, data analytics and AI can significantly enhance compliance processes, including TM. In tandem, regulators have also displayed an increasing openness to FIs implementing such techniques; for example, in December 2018, US regulators issued a joint statement to encourage FIs to consider innovative approaches to AML.[5]

FIs are designing AI tools to improve the identification of suspicious transactions and to refine the screening of Politically Exposed Persons (PEPs), sanctioned individuals and organisations. Until recently, FIs had heavily relied on rules-based systems for their transaction monitoring, which presented several limitations. However, FIs are now turning to machine learning to benefit from significant improvements in reducing the volume of false positives and increasing efficiency.

Applications of machine learning for AML transaction monitoring

Among the variety of different machine learning uses, the TM process presents a significant opportunity for application due to the solution's ability to make judgments and to identify behavioural patterns.

Risk rating suspicious behaviour, alert classifier and noise reduction

Machine learning algorithms can reduce false positive alerts by detecting suspicious behaviour and classifying alerts as being high, medium or lower risk following an RBA. Advanced machine learning techniques allow resources to focus on high-risk activity by automating the detection of alerts that are likely to require investigation and auto-closing alerts that are non-suspicious.

Anomaly detection and identification of transactional patterns

Machine learning techniques can identify patterns, data anomalies and relationships amongst suspicious entities that could have gone unnoticed under a rules-based approach.
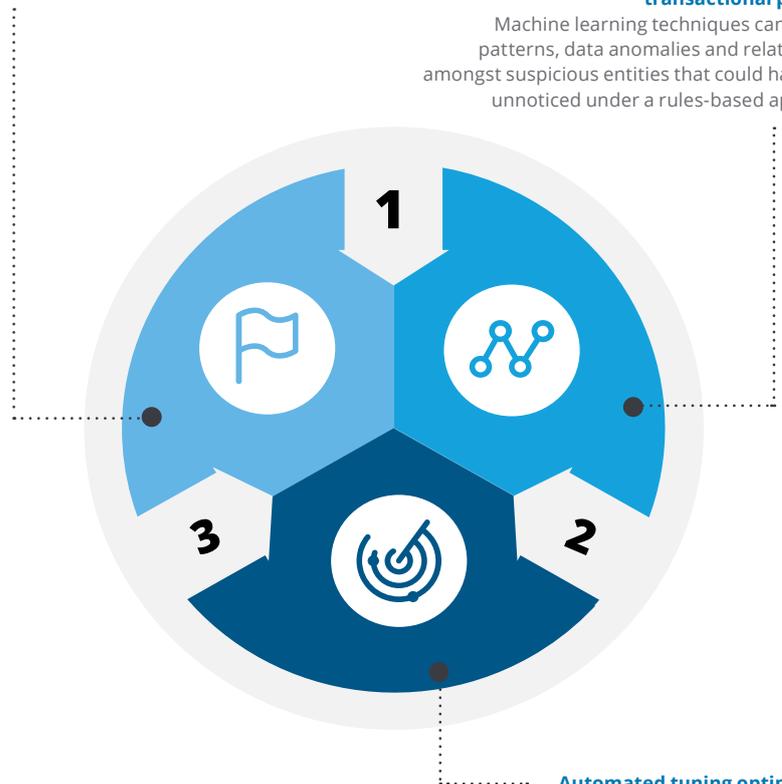
Automated tuning optimisation

Machine learning can run hypothetical scenarios to derive the optimal state for customer segmentation, rules and thresholds. Outcome review will determine if certain modifications are to be made in line with the FI's own risk appetite.

5. AIM Evaluation – Fraud and AML Machine Learning Platform Vendors, March 2019

Key considerations for the Transaction Monitoring journey

Whilst there are various benefits to be derived from embarking on a journey to optimise TM systems and many options through which this optimisation can be achieved, it remains vital that FIs examine some of the key considerations associated with each of these options to determine the most suitable method considering their organisation.

FIs must closely assess factors including data, technology, disruption, cost, time, long term savings, third party vendors and expertise against the organisation's current systems, resources and structure to make a fully informed decision.

Additionally, identifying where and how to embark on the AI and machine learning journey can feel daunting and complex. This, coupled with the competing pressures of BAU, emphasises the importance of clearly addressing these key considerations from the outset.

Whatever FIs eventually decide, it is vital that early engagement and eventual buy in of the senior management to explain the value proposition, the underlying problem statement and the cost estimates (including maintenance costs) is achieved.

Considerations	Improving existing systems	Introducing new technologies into the TM process
Data	FIs often experience issues around data quality, completeness and validity which have been typically addressed on a case-by-case basis such as alert and/or profile basis, or through large-scale costly data remediation exercises. To improve the TM process, FIs need to gain a comprehensive understanding of the data and eliminate potential obstacles to acquire the right data for analysis. The level of readiness for integration and application is dependent on existing data and systems in place. An assessment of the current systems and their operations will determine whether to replace, integrate or work around existing systems.[6]	
Technology	Desktop research and typology analysis are useful ways for FIs to enhance their TM framework without having to change the existing system/technology or other resources.	While some regulators are encouraging FIs to adopt new technologies to more effectively combat financial crime, focus on model transparency and explainable outcomes, it creates some obstacles for adoption of any new technology. An appropriate level of 'explainability' and transparency of AI and machine learning models and outcomes to relevant parties, especially regulators, is required to address the risks of 'black box' threat.[7]
Disruption	Desktop analysis and typology research is carried out in test environments and lead to minimal disruption, if any, as they primarily focus on improving existing technology in place and could be carried out alongside BAU activities.	The introduction of new technologies and systems could disrupt existing systems in place and may pose certain challenges with respect to BAU activities. There are several risks that arise from the use of new technology including but not limited to biases in inappropriate modeling techniques, flawed assumptions and incorrect interpretation of output.[8]
Cost	Improving existing systems is often the less costly option, as it does not involve large investments in technology or resources. This approach to optimisation is a quick fix that can help FIs improve their TM framework (at least for the short term) while remaining competitive in the market.	The introduction of new technologies and systems could involve significant costs and resources. Aside from the installation cost of these complex machines, the repair and maintenance also involve large costs with software programs requiring frequent upgrades.

6. Deloitte – Transforming Financial Crime Management through Technology, 2021
7. HKMA – Reshaping banking with Artificial Intelligence
8. Deloitte – Transforming Financial Crime Management through Technology, 2021

Considerations	Improving existing systems	Introducing new technologies into the TM process
Long term savings	Maintaining existing systems can pose some risks in the future considering the rise of dynamic data and sophisticated money laundering techniques. As a result, existing systems might process illicit transactions without the FIs' knowledge which could lead to regulatory breaches with legal, reputational and financial consequences. Furthermore, FIs will continue to spend on a large team of analysts required to review and close a large number of alerts.	The latest technology will allow more efficient use of data reducing the number of false positives and hence requiring a smaller group of people to review and conclude on the alerts generated. Furthermore, the use of technology will also reduce (if not eliminate) the cost of 'human error' involved in TM.
Third party vendors	TM optimisation has been carried out for a long time. A number of vendors have been using different methodologies and tools to improve the life of existing systems and have been successful as well.	When investing in a new technology/system, it is recommended that institutions consider the long-term viability of the vendor e.g. will the vendor (or their solution) remain valuable beyond an initial Proof of Concept (PoC)? Are the opportunities to scale? The same also holds true when selecting the latest technology for TM purposes. FIs should evaluate the compatibility of the vendor's size, scale and solutions with their organisation, systems and structure.[9] Moreover, FIs should evaluate the vendor's technical capabilities and expertise along with established experience and track record, including the maturity of the vendor and solutions, as well as financial sustainability. It is also recommended that the FI determines the intellectual property (IP) considerations prior to onboarding or co-developing solutions with third party vendors. Data handling and management with third party vendors should be completed in line with applicable data protection regulatory requirements across different relevant jurisdictions e.g. General Data Protection Regulations (GDPR).
Expertise	FIs have been undertaking TM for decades and have the expertise to continue to do so in its current state.	Recruiting the appropriate resources and expert talent who are knowledgeable about both AI and machine learning solutions and financial services, is at the heart of the success of adopting emerging technologies. It is necessary to build capabilities in understanding, validating and explaining how the models derive the recommendations to enable a successful use of the AI and machine learning solutions. FIs should provide extensive knowledge through trainings on how to best utilise the model outcomes and explain why specific predictions were made.[10] Quality documentation of the model and algorithms is required, as regulators expect FIs to explain how the models work including details on the technology and functionality, business requirements, outcome, risk mitigation approaches, testing and assurance.[11]

9. Deloitte – Transforming Financial Crime Management through Technology, 2021
10. Deloitte – The Case for Artificial Intelligence in Combatting Money Laundering and Terrorist Financing, 2018
11. Deloitte – Transforming Financial Crime Management through Technology, 2021

Glossary

ACAMS	Association of Certified Anti-Money Laundering Specialists
AI	Artificial Intelligence
AML	Anti-Money Laundering
BAU	Business as Usual
CBUAE	Central Bank of the United Arab Emirates
CFT	Combating the Financing of Terrorism
FATF	Financial Action Task Force
FI	Financial Institution
FIU	Financial Intelligence Unit
GDP	Gross Domestic Product
GDPR	General Data Protection Regulation
IP	Intellectual Property
KYC	Know Your Customer
LFI	Licensed Financial Institutions
MAS	Monetary Authority of Singapore
MiFID	Markets In Financial Instruments Directive
PEP	Politically Exposed Person
PoC	Proof of Concept
PPP	Public Private Partnership
RPA	Robotic Process Automation
SAR	Suspicious Activity Report
STR	Suspicious Transaction Report
TM	Transaction Monitoring
TMNL	Transaction Monitoring Netherland
UNODC	United Nations Office on Drugs and Crime

Key Contacts

Muzammil Ebrahim
Partner
Financial Crime Advisory
+97152 883 5537
muebrahim@deloitte.com

Saad Qureshi
Assistant Director
Financial Crime Advisory
+97156 524 5191
saqureshi@deloitte.com

Deloitte.