



While you
monitor
transactions,
who monitors
your transaction
monitoring
program?

■ ■ ■
The better the question. The better the answer.
The better the world works.



EY

Building a better
working world




Financial institutions (FIs) are pouring resources into transaction monitoring (TM), yet fines for poor TM practices are on the rise. As regulators focus on this key area of anti-money laundering (AML) defense, FIs are looking to harness new techniques to satisfy regulatory obligations while avoiding spiraling costs, both operations and regulatory.

TM is one of the key controls in an FI's AML risk management framework, allowing organizations to determine if a customer's behavior is potentially anomalous and has a potential AML and counter financing of terrorism (CTF) risk.

FIs have faced significant challenges in enhancing financial crime compliance (FCC) controls, which have typically been in

place for more than five years and undergone modifications because of increased regulatory focus. Additionally, in the last six months, TM fines¹ against FIs globally have continued to rise to hundreds of millions of US dollars, even for institutions that invested heavily to improve their AML TM programs.

1. Direct fines for breaches and cost of remediation activities



Although regulations differ from country to country, there are common trends in expectations from regulators and guidance to FIs to significantly enhance TM programs.

The goal posts have moved

Although regulations differ from country to country, there are common trends in expectations from regulators and guidance to FIs to significantly enhance TM programs.

What may have been acceptable to the regulators previously is no longer sufficient, as regulators expect a more nuanced monitoring approach that is reflective of the financial crime compliance risk faced by the banks:

Previously	Current and emerging practices
------------	--------------------------------

- | | |
|--------------------------|---|
| One-size-fits-all | <ul style="list-style-type: none">▶ Monetary Authority of Singapore (MAS)▶ Localized monitoring: FIs can no longer blindly implement head office scenarios or parameters. They need to examine thresholds at an individual country and division level, considering the risk profiles of local businesses and customer bases, while accounting for the products and services, which are being facilitated. |
| All risks are equal | <ul style="list-style-type: none">▶ Hong Kong Monetary Authority (HKMA)▶ Australian Transaction Reports and Analysis Centre (AUSTRAC)▶ Risk-based approach to monitoring: Rather than putting the same parameters around monitoring all customers, FIs need to structure monitoring on the basis of risk level. Customers at different risk levels need their own scenarios which ensure that customers presenting the highest levels of risk receive more scrutiny. |
| Account-level monitoring | <ul style="list-style-type: none">▶ MAS▶ HKMA▶ AUSTRAC▶ Holistic monitoring: When FIs only monitor at an account-level basis, they often miss out on the bigger picture information that may have impacted their assessment of the alerted transaction. A consolidated, single customer view lets investigators assess the conduct of an account holistically and consider the risks of the overall customer relationship. This is especially important when dealing with high-risk customers and politically exposed persons (PEPs). |

As a result of regulatory inspections, banks have been penalized for:

- ▶ **Poorly calibrated TM systems**
 - ▶ Gaps in monitoring – examples of which include missing transactions, data quality issues, invalid mappings and gaps in scenario coverage (including local and regional risks)
 - ▶ Lack of documentary evidence to rationalize scenarios and thresholds chosen
 - ▶ Scenario coverage and thresholds not being reassessed since initial implementation
 - ▶ Risk-based approach not clearly justified
 - ▶ Capped generation of system alerts, typically on the basis of operational capacity rather than risk tolerance
- ▶ **Inadequate TM investigation practices**
 - ▶ Insufficient and inconsistent investigation documentation
 - ▶ Insufficiently trained investigation staff
- ▶ **Lack of regular testing and assessment**
 - ▶ Lack of a risk assessment to ensure there is adequate coverage to mitigate the AML risks that FIs are exposed to
 - ▶ Lack of statistical analysis to justify thresholds settings
 - ▶ Lack of a proper monitoring of critical data elements for data quality and completeness

Questions for TM system owners

- ▶ When was your system last reviewed?
- ▶ Are your TM system and scenarios properly configured for your product and client mix?
- ▶ Is your TM program effective, meeting regulatory obligations and mitigating the AML/CTF risks your institution is exposed to?
- ▶ What is the projected alert volume increase after any changes to your system? And do you have sufficient capacity to manage it?
- ▶ How good is your data quality and completeness for your TM system to run effectively?
- ▶ Are you able to extract key performance indicators (KPIs) and key quality indicators (KQIs) to enable you to monitor and enhance your TM systems?
- ▶ Can your IT infrastructure support current and future TM data volumes?
- ▶ Have you evaluated how emerging technology, analytics and RegTech could help improve your end to end TM processes?

How to meet regulators' expectations

1. Improve quality in existing TM systems

As a first step, FIs need to conduct a detailed review of their TM program and systems to determine if it is effective based on industry practices, regulatory expectation and their risk profile. This will increase the effectiveness of monitoring and assist in reducing false alerts. FIs need to ensure they have:

- ▶ **A well-configured TM system:** To better comply with regulatory expectations and to increase alert-to-case ratios, the TM system and processes need to be adequately designed and calibrated to address risks that the FI is exposed to on the basis of the size and complexity of its customer base, and transaction volumes:
- ▶ **Type of clients:** What is the risk profile of our customer base and how does it align with the bank's risk appetite? Has customer segmentation been performed to determine where the greatest potential risk areas exist?
- ▶ **Type of transactions:** What is the nature of the transactions currently being captured by the TM system? Does this align with the business units and divisions, customer type and products and services provided by the bank?
- ▶ **Geographical risk:** What is the geographical risk profile of these transactions? Are transactions conducted to or received from high-risk jurisdictions being adequately monitored and flagged by the TM system?

► **Quality data:** Monitoring systems are only as good as the data fed into them. Robust data quality programs should be applied to TM systems to ensure that the rules engines are making decisions based on the right information. In addition, data completeness is a common problem whereby not only is there a gap in providing critical data elements for the transactions being reviewed, but in some cases, there are upstream systems and even entire businesses or divisions not being run through the TM review process.

► **Regular calibration in place:** With AML risks constantly evolving, regulators expect FIs to give priority to the continual enhancement and maintenance of its TM systems. It is vital to perform regular AML risk assessments, and use model validation techniques, such as above- and below-the-line testing to regularly check thresholds and parameters so that the TM system remains effective in its ability to identify unusual transactions.

► **Well-trained staff:** No matter how well-calibrated a TM system is, it can always be undermined by its operators. The TM staff needs guidance on identifying risk patterns in client profiles and regular training on new AML risks; ultimately, the TM staff needs to understand the AML risks that its FI faces.

Traditional techniques have limitations

Many banks are already in progress or have executed their plan, particularly those who have been subjected to regulatory scrutiny. They have invested heavily to address shortcomings, mostly using traditional techniques to improve effectiveness, including introducing additional monitoring rules in systems.

Even with these changes, there is common agreement in the industry that the current TM infrastructure has limitations. TM processes remain largely manual, creating a large volume of alerts typically with high false positives rates (over 90%),² which require hundreds of human resources to spend time on largely unproductive and costly endeavors.

2. Harness technology and analytics to improve both efficiency and accuracy

Faced with growing costs to meet regulatory obligations, many FIs are looking to improve risk management and drive efficiencies, while saving costs using technology and analytics.

Analytics for parameter setting: Use sound statistical techniques based on historical data to calculate and validate parameters in AML models (i.e., AML TM rules and segments) to achieve an optimal level of control effectiveness, while reducing false positives and improving system performance.

Automatic data collection and enrichment: In manual TM systems, human investigators often spend 70% of their time gathering and formatting data³. Why not have the investigators focus on decisioning tasks rather than manual repetitive tasks? Automation techniques, including robotics⁴, digitalization of information⁵ can reduce TM resourcing constraints by assisting investigators to automatically gather and structure information. Additionally, automation can help reduce inconsistencies by automatically documenting part of the investigation narrative. These structured narratives have the additional benefit of providing better data points for potential artificial intelligence (AI) and machine learning (ML) models.

Decision support models: Advanced analytics, such as AI and ML models can greatly enhance TM decision support. As you feed more TM-related data into these tools, models can learn to score alerts, prioritize material alerts that investigators should investigate and identify potential alerts for automatic disposition. Today, analytics will not completely replace human investigators in the TM process, instead, it may augment existing TM controls by processing historical customer and transactional data to identify trends or anomalies that aid in the prediction of potential suspicious activity.

Alternative models: Secondary monitoring is increasingly used on top of existing TM systems. Some FIs are beginning to implement detection mechanisms using alternative approaches to rules-based monitoring. Dedicated analytics teams (with in-house or external resources) are developing and modifying rules based on identified risks – rather than just relying on traditional rules-based technologies. Some of these approaches are specific to a certain typology or detection pattern, e.g., upstream customized analytics for money mule detection. Already, analytics are helping FIs to identify activities that flag human trafficking, tax evasion and other financial crime-related typologies. It's yet another facet of combating financial crime.

2. "Detailed analysis," *Anti-money laundering (AML) Transaction Monitoring 2018 EMEA Survey Report*, October 2018, EY, 2018.

3. On the basis of a time-motion study of AML TM, Level 1 investigations at a global multinational banking and financial services company

4. Process automation (attended) and desktop automation (unattended)

5. E.g., optical character recognition (OCR) for document scanning

Case study



Problem statement

A large multinational institution was facing an imminent increase in alert volumes and required a solution to be deployed rapidly to reduce investigation time, while maintaining investigation quality.

- ▶ The number of "Level 1" transaction monitoring alerts was very high and known to be increasing due to configuration changes (including new monitoring scenarios) required to meet regulatory expectations.
- ▶ An increase of 50% in relevant full-time employees (FTE) would be required to manage the projected alert increase.
- ▶ The bank wanted investigators to focus on the investigation itself rather than information gathering from multiple sources.


EY services

EY teams were responsible for the following activities:

- ▶ Design a solution, which will help deliver innovative capabilities to support the AML TM Level 1 alert investigations operation using an automation, advanced analytics and technology solution
- ▶ Build the solution using industry leading software suite, and extract data from the clients' AML TM system and third-party data sources
- ▶ Help lead implementation, continuous improvement and rollout to multiple geographies
- ▶ Provide support to execute user acceptance testing (UAT) and training activities
- ▶ Handover and support the client's technology teams to configure and rollout the solution to additional countries independently from EY teams, once the product was in business-as-usual and had been deployed to the propriety countries in scope

Results

- ▶ Approximately 50% reduction in time to complete an AML TM alert investigation at Level 1
- ▶ Initial solution, build and deployed into production in less than six months
- ▶ Solution deployed to multiple geographies, supporting three languages
- ▶ Improvement in efficiency (throughput), effectiveness (accuracy) and quality of investigations
- ▶ Leveraging data to provide the client insight and intelligence feedback to upstream processes
- ▶ Identification of additional AML red flags not identified by the primary monitoring system
- ▶ Investigation quality improved, and current process irregularities highlighted being accepted by quality assurance (QA) team



Banks are continuing to focus on TM not only as a key area to enhance the monitoring of their financial crime risk but also as one of the greatest areas of weakness for regulatory compliance. A significant amount of time and money is being invested to uplift this capability as it tends to be a heavily manual function with little value-add being applied. The result is a combination of innovative solutions and good business hygiene to provide greater visibility into the risks each customer and their transactions expose the bank and the financial system at large to.

Contacts

**David Scott**

EY Asia-Pacific Financial Crime
Compliance Leader
+852 2629 3070
david.scott@hk.ey.com

**Samuel Lung**

EY Greater China Financial
Crime Compliance Leader
+852 2675 2116
samuel.lung@hk.ey.com

**Maggi Hughes**

EY ASEAN Financial Crime
Compliance Leader
+65 6309 8268
maggi.hughes@sg.ey.com

**Scott Mandell**

EY Oceania Financial
Crime Compliance Leader
+61 4 2682 9423
scott.mandell@au.ey.com

EY | Assurance | Tax | Strategy and Transactions | Consulting

About EY

EY is a global leader in assurance, tax, strategy, transaction and consulting services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. For more information about our organization, please visit ey.com.

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax, legal or other professional advice. Please refer to your advisors for specific advice.

ey.com

© 2020 EYGM Limited.
All Rights Reserved.

EYG no. 002419-19GbI

BMC Agency
GA 1010768

ED None