



## Fit-for-Purpose Transaction Monitoring: Tackling financial crime head on

# Transactions Monitoring – Tackling financial crime head on

By Simon McMahon and Victoria Kelly



With less than 1% of alerts detecting genuine threats, transaction monitoring is in need of an overhaul. The FCA's recent 'Dear CEO' letter for retail banks underlines the need to take action. How can your business turn this currently blunt tool into a targeted and efficient, risk-first weapon in the fight against financial crime?

Transaction monitoring (TM) should be a vital part of the financial crime control framework, helping to unearth suspicions of money-laundering, and terrorist financing.

All too often, however, the generic way the automated systems are set up means that they generate a vast number of false positive alerts, while failing to detect a significant amount of genuinely suspicious activity. Typically, less than one in a hundred alerts highlight authentic risks. Nonetheless, regulation requires that all these alerts are investigated, which ties up operational resource that could be far better used in tackling real threats.

## Common failings

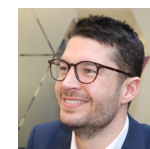
Why are systems missing the mark? Most 'off the shelf' applications are focused on the need to demonstrate compliance rather than the financial crime risks within a particular organisation. They comprise rules which may not even be applicable to the specific transactions, products and client services offered by the organisation.

Many of the monitoring systems utilised use broad brush triggers, such as high or unusual deposit levels, rather than honing-in on the ways in which financial crime is actually carried out. Much greater customisation is required.

## FCA's continued spotlight on TM

The urgent need to address these shortcomings has been heightened by May's *Dear CEO* letter from the FCA. The FCA's concerns range from "arbitrary thresholds" to solutions that "have not been calibrated appropriately for the business activities and underlying customer base".

Our 'Check list of common weaknesses in TM' at the end of this article outlines the common failings, their causes and the outcomes. This can help inform the gap analysis retail banks must undertake to meet FCA obligations. The big question is, of course, how to address these shortcomings.



**Simon McMahon**  
Senior Manager  
[simon.mcmahon@baringa.com](mailto:simon.mcmahon@baringa.com)



**Victoria Kelly**  
Manager  
[victoria.kelly@baringa.com](mailto:victoria.kelly@baringa.com)

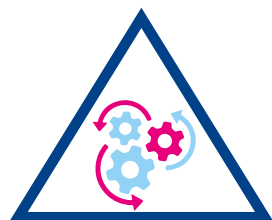




# Three ways to get up to scratch

At Baringa, we've been looking closely for several years at how to get systems up to scratch.

For us, the key is ensuring that TM is configured according to the underlying risks of the organisation, and utilising all available information about a customer's behaviour to identify them accurately. What then are the key features of this fit for purpose TM? Three priorities stand out:



## 01 Optimise the basic configuration

The most fundamental aspects of TM configuration are the scenarios (or rules), the customer segmentation model and the thresholds. Together, these define when an alert should be created for each scenario-segment combination.

Appropriate methodologies should be defined and executed to optimise these fundamentals. They should also harness all relevant bank data. If executed appropriately, this should lead to a system which is much more readily able to identify potentially suspicious activity.

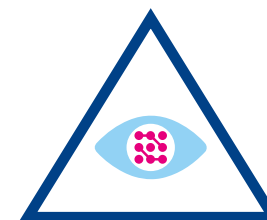


## 02 Implement a secondary analytics engine to refine existing output

Whilst a well configured 'traditional' TM system may identify a greater proportion of potentially suspicious behaviour, it will still generate a lot of false positive alerts and miss a significant proportion of the behaviour it is intended to identify. Secondary analytics can help to refine the outputs by weeding out the false positives and more accurately pinpointing suspicious behaviour.

However, the suggestion that a machine learning model, in itself, will provide the answer, is likely to be an empty promise.

It is much more important that the pertinent pieces of information about a customer's behaviour are identified in order to contextualise their behaviour and determine whether it is likely to be suspicious or not. Such information can be used to significantly improve the accuracy of rules-based models, or act as the 'features' of machine learning models. Either way, the end-result will be much more effective than traditional TM systems. We've adopted this contextual monitoring approach within the 'Triage' module of our Typify™ solution. This can cut false positive alerts by half, while also dramatically improving the detection of truly suspicious activity.



## 03 Streamline the investigation process

The information required to carry out an effective financial crime investigation, as well as the associated processes and workflow is often overlooked by traditional TM systems. Focusing on what an investigator needs to undertake a best-practice investigation can significantly improve the effectiveness and efficiency of your financial crime operations. Areas of improvement include:




- ▲ **Leveraging all of the pertinent information available about a customer** to make a more informed decision – this can include data from other internal systems, as well as data from third parties that helps to contextualise a customer and their behaviour.
- ▲ **Visualising information to ensuring it is easily digestible** by using customisable infographics rather than raw data. For example, providing an interactive tabular and graphical summary of the customer's transactional activity for the prior year, rather than a static list of their recent transactions.
- ▲ **Identifying additional risk indicators that either increase or decrease suspicion** associated with a customer's behaviour – traditional systems are often quite one-dimensional in consideration of a customer's behaviour and such indicators can help to much more accurately qualify whether it is likely to be suspicious.
- ▲ **Consolidating multiple alerts that relate to the same customer.** This prevents needless duplication of effort in looking into the same issues.
- ▲ **Automatically generating the investigation narrative** – providing comprehensive documentation of the customer's behaviour and the investigation, to be verified and revised by an investigator, rather than requiring them to write this from scratch.

## Confidence in your TM

Automated TM is here to stay. But there are serious gaps and regulators want them addressed.

Trying to find genuine suspicious activity in a sea of alerts also uses up needless time, money and resources. Bringing your system up to scratch demands both sharper risk identification and refinement of system outputs to enable these risks to be investigated efficiently. Our risk-first approach to TM will help to give both your regulator and your board confidence that your systems are identifying all relevant types of suspicious behaviour. It does this by focusing on the ways in which criminals may actually attempt to exploit your organisation and tackles them head-on.

## Checklist of common weaknesses in transaction monitoring

| Challenge Type   | Challenge  | Issues we commonly see  |
|--|--|---|
| <b>Effectiveness</b><br>                | Providing appropriate and complete data to the TM system                                 | <ol style="list-style-type: none"> <li>1. Certain transactions are excluded from the TM data feed, preventing a complete picture of transactional behaviour being monitored.</li> <li>2. Provision of the 'minimum viable' data to a solution, preventing the curation of targeted scenarios and limiting available information for subsequent investigation.</li> </ol>  |
|  | Ensuring TM rules/scenarios are tailored to the underlying risks specific the bank       | <ol style="list-style-type: none"> <li>1. Group-led TM solutions being used for local subsidiaries without being appropriately calibrated.</li> <li>2. Using 'off-the-shelf' scenarios and accompanying thresholds with limited rationale of how this is relevant for a firm's underlying risks and expected levels of customer activity.</li> </ol>  |
|  | Calibrating the system to detect activity worthy of investigation                        | <ol style="list-style-type: none"> <li>1. Lack of an understanding of how a system can be effectively tuned.</li> <li>2. Absence of customer segmentation.</li> <li>3. Scenario thresholds that are set arbitrarily or simply to meet operational capacity.</li> </ol>  |
| <b>Effectiveness and Efficiency</b><br> | Providing the necessary information to facilitate a comprehensive investigation          | <ol style="list-style-type: none"> <li>1. Long investigation times, with investigator's time spent gathering additional information required to make a decision.</li> <li>2. Insufficient rationales provided when discounting alerts.</li> </ol>   |
|  | Developing effective MI to inform and improve system                                     | <ol style="list-style-type: none"> <li>1. No understanding of which detection scenarios are operating effectively.</li> <li>2. Alert outcome information not being captured effectively and not being used to improve scenarios.</li> <li>3. Limited understanding of investigation team productivity, and which areas require improvement accordingly.</li> </ol>  |
|  | Maintaining the system appropriately   | <ol style="list-style-type: none"> <li>1. Poor governance that does not mandate senior management approval for configuration changes and does not require continuous improvement.</li> <li>2. Lack of sandbox environment in which to test new/modified scenarios outside of production.</li> <li>3. Lack of agility to respond to issues, new regulatory requirements and emerging threats – exacerbated by complexity of vendor solutions.</li> </ol> |
| <b>Efficiency</b><br>                 | Defining an appropriate investigation process  | <ol style="list-style-type: none"> <li>1. Full account/customer reviews completed, rather than focussing on the Financial Crime risks highlighted by the triggered scenario(s).</li> </ol>  |
|  | Consolidating alerts appropriately   | <ol style="list-style-type: none"> <li>1. Multiple alerts related to the same customer (e.g. related to different accounts, different scenarios, or generated from a different system) are investigated separately. This causes duplication of effort, as well as reducing the effectiveness of investigation by not considering alerted risks holistically.</li> </ol>   |
|  | Calibrating the system to avoid large volumes of false positives (i.e. worthless alerts) | <ol style="list-style-type: none"> <li>1. Very low alert escalation rate following investigation, with less than 5% considered 'worthwhile'.</li> <li>2. Investigator fatigue as a result of the ratio between worthless and worthwhile alerts.</li> </ol>  |

# About Baringa Partners

Baringa Partners is an independent business and technology consultancy. We help businesses run more effectively, navigate shifts and reach new markets.

We use our industry insights, ideas and pragmatism to help each client improve their business.

Collaboration is central to our strategy and culture, ensuring we attract the brightest and the best. And it's why clients love working with us.

**Baringa. Brighter together.**

**Baringa Partners LLP**

62 Buckingham Gate  
London  
SW1E 6AJ  
United Kingdom

+44 (0)20 3327 4220  
[enquiries@baringa.com](mailto:enquiries@baringa.com)

[baringa.com](https://baringa.com)

