Synechron

# What's Going on in the World of Transaction Monitoring?


Authored by:

**Bas Uildriks**
Consultant and Transaction Monitoring Expert
Synechron, The Netherlands


Transaction Monitoring (TM) is an important weapon in your fight against Financial Crime. After seeing dozens of implementations of TM systems, varying from good to adequate to a fear mongering 1000-false-positives-per-day-generating-machine, I would like to touch on a couple of insights.

There are multiple best practices and bad practices. For example, the assumption that using a smaller number of scenarios or rules will result in a reduced number of alerts (simply a false assumption and a bad practice). But there are techniques which actually contribute to lowering false positives, like applying peer grouping in your customer groups, and creating backstop rules -- but only with a proper data analytics process to support this.



# Don't Struggle: Leverage the Power of Data

I still see lots of banks struggling with a good implementation of their TM system(s). So, what can you do about this? The good news is that you're not alone, and the problem has been solved numerous times already. It all starts with data. The quality is important, but also the mapping of financial and non-financial data towards values used in the TM system is key and must be fully understood. Then, with the data side of things sorted, the fun part starts.

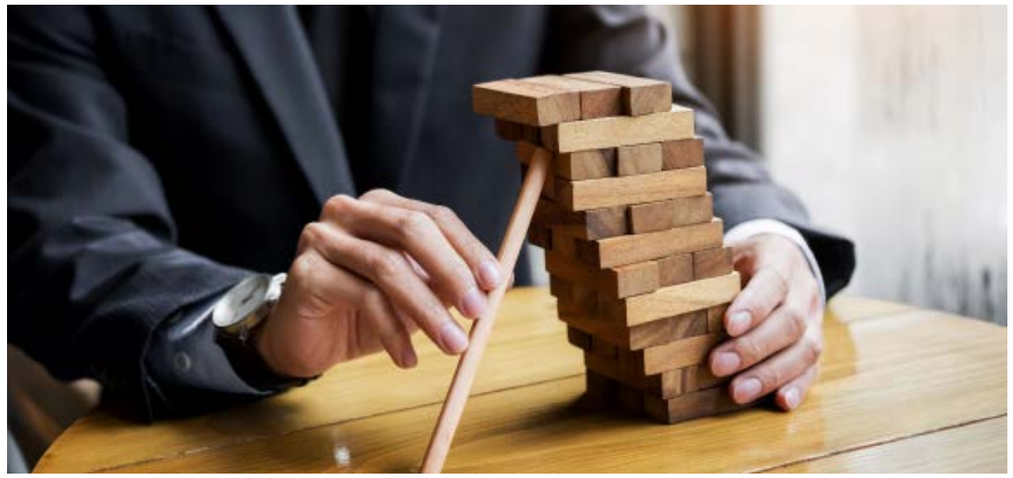
Based on your risk appetite, size of the operational teams and business logic the (re-)design of the TM system starts. Vendors sometimes offer an a-la-carte menu of rules sets/models. However, if you decide to use these you need to understand them from A to Z.

TM for Fraud and AML are two different things. For AML, TM is typically done post-transaction (after the fact) while TM for Fraud is real-time and in blocking mode. Current trends are applying Artificial Intelligence (AI)/machine learning to predict malicious behaviour and to find the outliers based on historical data.

The FinTech world is booming, but so is the payment landscape with revised Payment Services Directive (PSD2) EU directive and OpenBanking. Speed is of the essence, so it's worthwhile to jump on the bandwagon!

> It's important that you can explain in simple terms what your mitigating actions are and how these are translated into the rules or models running in the TM system.

# Applying a Risk-based Approach to Transaction Monitoring



Ever since the Financial Action Task Force (FATF) came out with its 40 recommendations, everyone in the AML/fraud domain has dealt with a Risk-based Approach (RBA). But it's not that easy to map specific scenarios towards specific risks. Further, and especially towards the regulator, it's important that you can explain in simple terms what your mitigating actions are and how these are translated into the rules or models running in the TM system.

**You should ask yourself:**

- Does this specific rule map to a specific risk you have identified in the RBA?
- Do the alerts which are being generated contribute to mitigate this risk? Nine out of 10 times the monitoring systems contain lots of these 'rogue' or legacy scenarios.
- What can you replace these pesky scenarios with?

Using an RBA is actually a good starting point, including taking steps like identifying customer, channel and product groups, and doing a risk scoring exercise on each intersection. In this way you can design your logic with a specific focus. Also check other mitigating actions like staff training, certification and knowledge sessions. These will all help you to start monitoring the identified area of risk so you will regain control.



# How to detect Money Laundering with Transaction Monitoring?

Transaction monitoring against money laundering needs to be explanatory and fully transparent. That's why rule-based systems are still favored over machine learning/AI systems; because you need to explain to the regulator how this intelligence is working in a coherent way with the Risk-based Approach. A big misconception is that if you have fewer scenarios they will result in fewer alerts. Actually, the opposite is true. If you create more variances of specific scenarios, you will be able to use more variables and can tweak these variances in the normal deviations you encounter as part of the day-to-day operation of your bank. The successful TM systems I've seen applied the logic clustered per business line and applied peer grouping on customer groups (age, income, geography). This sometimes results in hundreds of business rules which can be tested, tweaked and deployed and are the result of statistics gathered by data scientists.

> Transaction monitoring for AML should be fully transparent to your regulator and so easy to explain, that even your mother could understand it.

My key takeaway here is that transaction monitoring for AML should be fully transparent to your regulator and so easy to explain, that even your mother could understand it. If you're new or have a blank canvas TM project, then start per business line and scale-up quickly after the first stage, based on the learnings from that stage.

# How to detect FRAUD with Transaction Monitoring?


Technology facilitates endless possibilities in scalability and speed. From the early days, where mainframes spat out printed lines of 'alerts', technology has helped the TM area tremendously over the last few decades. Models used in the card space based on limited data features have set the standard. Relational databases helped us in gaining holistic views of customers and their activities on the account/customer level, but also on the counterparty (beneficiary) level. Now, with migration to the cloud and the increased speed and low cost of computations fighting Financial Crime will become even better.

If you are attending any online seminar or roundtable on TM these days, then you probably can't see the forest for the trees. Buzz words, like artificial intelligence, machine learning and data science will be tossed about, but how will these actually help you? The answer is not as straightforward. Machine learning models are nothing new, but they are very good at predicting values or series for a specific purpose. And, when it comes to fraud, the effort is driven by the business case and reputational damage and not so much on regulatory pressure.

I recommend to test as much as you can, and try and experiment with every possibility you have. Start a Financial Innovation Lab (FinLab) environment and invite creative FinTechs to apply their ideas and creativity to your specific business and its needs. Have a working sandbox environment with transactions, accounts and customers which behave in a real-world kind of way. Only then can you measure the true potential of this new generation.

> **Have a working sandbox environment with transactions, accounts and customers which behave in a real-world kind of way.**



# But what about Advanced Persistent Threats (APT)?


The arms race on fraud fighting technology also goes for our adversaries who commit fraud: the bad guys. The groups responsible for Advance Persistent Threats (APT) are either private or state sponsored. They're equipped with custom toolkits tailored to your financial institution, with a financial gain or reputational damage as their primary goal. APT groups have more time, greater resources and probably better skills than you and your team have. So how will you maintain leverage against such bad actors?

There's lots to gain on the intersection of cyber security and fraud. So called Fusion Centres are on the rise, where data from the Security Operation Centres (SOC) is combined with transactional data, like money leaving the bank. Combining those data points from financial events with non-financial events in real-time demonstrates that you can easily predict your 'normal-abnormal' behavior of your financial institution.

Finding the common denominator is key; doing it in a fusion-kind-of-way is not that difficult. It entails just getting the data which will work for you. The proof is in the pudding. Feature selection is the obvious challenge here, but once mastered you'll be vastly more resilient against events which don't come along often but are of high impact. Armed with this insight on the 'normal-abnormal' behavior, you will be able to respond to a black swan event by only taking down transactions based on this common denominator, while the rest of the bank stays open.

**Bas Uildriks**
Consultant and Transaction Monitoring Expert
Synechron, The Netherlands

Bas Uildriks is a Consultant with Synechron, The Netherlands, and a subject matter expert in Transaction Monitoring (TM). He has implemented dozens of TM solutions globally and has worked for FinTechs, insurance companies, payment service providers, banks and their regulators.

Want to learn how Synechron can assist you in getting control over your TM system? Let's get in touch!

Reach out to:
Bas.Uildriks@Synechron.com


www.synechron.com