Compliance Monitor
Business intelligence | informa

www.compliancemonitor.com

COMMENT › TECHNOLOGY

# Pitching machine intelligence against financial crime

The precise application of machine intelligence solutions can enhance existing technologies and processes to detect potential financial crime, without the need to engage in large-scale software upgrades. **Alma Angotti**, **Timothy Mueller** and **Joe Campbell** explain how 'MI' can help with segmentation, prioritisation and typology development.

## Introduction

Anti-money laundering (AML) transaction monitoring (TM) to identify potentially suspicious transactions is a challenging undertaking for banks and other financial institutions. It is an important tool to stop the funding of terrorist activity, money laundering, as well as other crimes such as human trafficking and drug distribution. Yet existing AML TM systems and processes have proven to be operationally inefficient and often ineffective.

Machine intelligence solutions (which includes cognitive computing, artificial intelligence, machine learning, and deep learning (collectively MI)) can enhance existing technologies and processes to detect possible financial crime better. The precise application of these technologies can deliver significant efficiencies without the need to engage in large-scale software upgrades. As a result, leading financial institutions, with industry partners, have started to deploy MI against the complex challenges presented by AML and TM in particular.

## Why traditional AML TM solutions are increasingly ineffective to fight financial crime

Detecting financial crime with AML TM is inherently difficult because it involves complex transaction data, often disconnected systems, and substantial human involvement. These issues are amplified for large, geographically diverse financial institutions.

The challenges begin with the number of investigations. As the rigour applied by financial institutions and regulators is increased to address more fully the risks and red flags associated with the products, services and geographies of the business, so does the volume of alerted transactions that a financial institution must investigate. Banks and other financial institutions are aware that many, indeed most, of these timely and costly investigations do not result in the identification of potentially suspicious activity, and therefore these efforts are ineffective and inefficient.

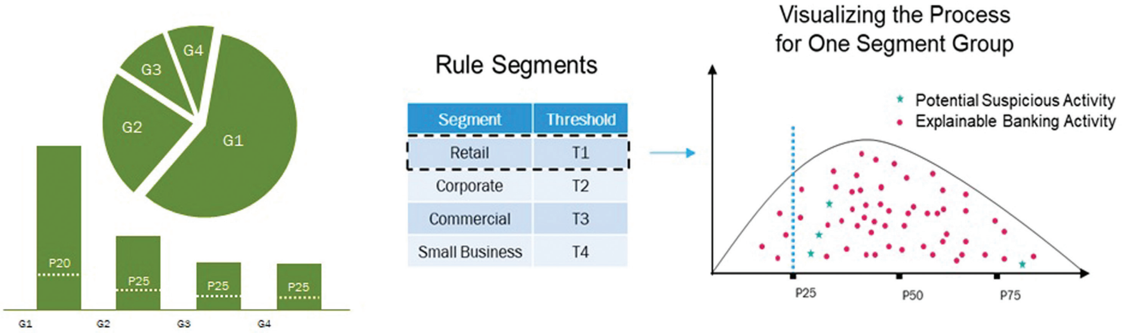
Banks and other financial institutions are also aware that the heart of the problem is finding the balance between signal and noise. Too many alerts that represent normal banking activity or 'noise', is inefficient. Too few alerts may mean that the bank is missing potential criminal activity and is exposed to unknown risks.

These issues stem from three primary inefficiencies:

a. Most AML TM processes typically have predefined and static money-laundering rules or detection scenarios.
b. Most AML priority or triage programmes use time-based, amount specific, or rule scoring to prioritise investigations.
c. Risk typologies are often limited to known behaviours rather than emerging risks.

Financial institutions can and should re-imagine these processes using MI. This requires a principled approach that combines subject matter expertise, knowledge of regulatory expectations, and proven experience applying MI techniques to large data sets.

Traditional segmentation



| Segment | Threshold |
|---|---|
| Retail | T1 |
| Corporate | T2 |
| Commercial | T3 |
| Small Business | T4 |

1. Segments not adequately distributed.
2. The thresholds set are often too low, and result in many false positives.

To alert on the potential suspicious activity of this segment, a lot of explainable behavior also needs to be reviewed.

## Guiding principles for MI implementations

Regulators have indicated they are open to the application of MI in compliance functions, but they have been clear that cost reduction should not be the sole focus. To facilitate a successful implementation, certain guiding principles should be followed. These include:

### Start small

Have a clear objective. If specific areas are targeted first, a proper testing plan, controls, and success criteria will be easier to develop. Lessons learned can then be carried forward to other areas. In addition, the inevitable technology integration hurdles will be easier to overcome.

### Be transparent

No ‘black box’ solutions. Regulators, audit and model-testing teams need to be able to access and understand deployed solutions.

### Ensure effectiveness

AML risks must be adequately addressed and mitigated. Improvements in process must be demonstrable. This can be achieved in a variety of ways, including a reduction in false positives or an increase in identified data-driven high-risk events.

### Justify

Subject matter experts should review and test as well as independently validate deployed solutions.

### Use proven technology

Solutions and vendors with a track record of deployment will have already undergone multiple rounds of review and vetting. Choosing the right technology and compliance partners is essential.

### Augment existing processes

Developed MI solutions should support current systems instead of being viewed as a direct replacement.

## Identifying the right team

Whether an internal team or an industry partner, the right team is crucial for deployment of MI effectively and efficiently within an existing compliance programme that is consistent with regulator expectations and regulatory trends.

First, extensive AML subject matter knowledge is needed to guide the solution development process, as well as to provide thorough testing to verify predicted outcomes. For example, an alert prioritisation model might be developed through MI, but the basis for the prioritisation will need to be evaluated to ensure there is a relationship with known AML risks, and the prioritised alerts will require investigative testing to ensure that forecasted results are accurate.

The next requirement is a cutting-edge technology platform and an associated team that has a proven and tested track record of deployment specific to the institution’s needs. For example, a model that has previously been developed to ingest wire data or Society for Worldwide Interbank Financial Telecommunication (SWIFT) message formats will require less upfront work than an MI platform developed for web-based customer analytics.

Lastly, working with a team that has implemented and tested MI solutions in a compliance context gains credibility with regulators and ensures the alignment of risk coverage and deployed solution. MI applications in financial crime compliance are only as good as the team implementing and using them.

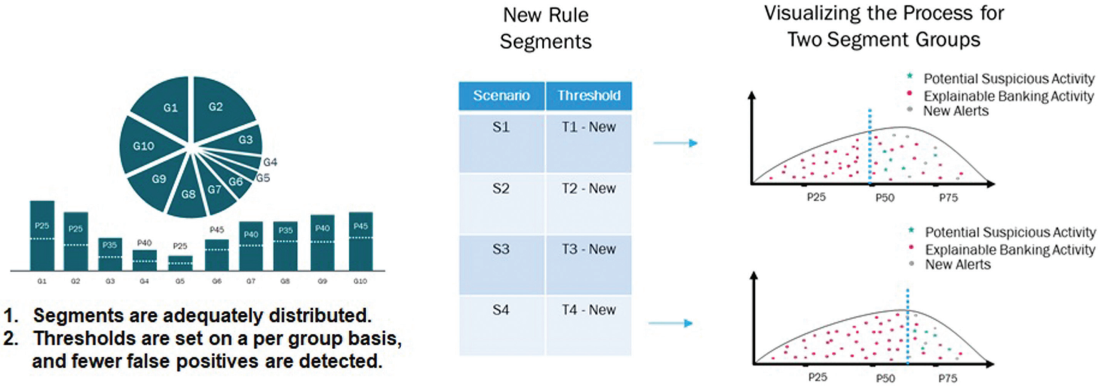
## MI in AML transaction monitoring

While AML MI solutions can cover a broad range of areas, there are three entry points that satisfy the ‘start small’ approach and can each be implemented alone or in combination. These include customer segmentation, alert prioritisation and typology development.

### Segmentation

A significant driver of the false-positive problem in AML is poor segmentation of customer populations. Even financial institutions with advanced segmentation models can suffer from over-inclusive segments that generate high false-positive rates, as well as high false-negative rates.

**Intelligent segmentation**


G1
G2
G3
G4
G5
G6
G7
G8
G9
G10
P25
P25
P35
P40
P25
P45
P40
P35
P40
P45
G1
G2
G3
G4
G5
G6
G7
G8
G9
G10
Potential Suspicious Activity
Explainable Banking Activity
New Alerts
P25
P50
P75
Potential Suspicious Activity
Explainable Banking Activity
New Alerts
P25
P50
P75

1. Segments are adequately distributed.
2. Thresholds are set on a per group basis, and fewer false positives are detected.

New Rule Segments

| Scenario | Threshold |
|---|---|
| S1 | T1 - New |
| S2 | T2 - New |
| S3 | T3 - New |
| S4 | T4 - New |

Visualizing the Process for Two Segment Groups

### *Traditional segmentation*

Traditional segmentation is typically based on customer risk rating, industry, or a classification such as retail versus commercial. These approaches are static and unrefined because they only consider a limited set of factors, and much of the data that is leveraged is a poor proxy for transaction activity. Moreover, the segmentation is often performed manually and separately for customer data and transaction data. The result is an inability to capture complex data interactions effectively.

These weaknesses in segmentation have a massive effect on downstream operations and processes when unrefined segments and inflated thresholds converge in the TM system.

A typical segmentation process produces irregular groups and leads to thresholds being set artificially low for the population – resulting in a significant number of false positives.

When AML rules are triggered, the alerted transactions must be investigated and dispositioned. The result is significant operational risk from a large investigations team processing large numbers of alerts.

### *Intelligent segmentation*

MI can be used automatically to assemble similar groups of customers and customers of customers. This results in more granular and uniform segments and, thus, in correctly set thresholds without sacrificing the risk of omitting potentially suspicious transactions.

A qualitative approach should be applied to verify any identified segments by performing investigations of alerts and comparing against projected outcomes. This ensures expected results are in line with real-world performance.

## Alert prioritisation using machine intelligence

As banks and other financial institutions have got better at monitoring their transactions for potentially suspicious behaviour, the number of alerts and investigations has only increased. To address this, a variety of prioritisation approaches have been deployed. This prioritisation is usually based on time, dealing with the latest alerts first, or some form of rule-based scoring. The prioritisation model can be enhanced using MI.

MI can be used to accelerate clearing of alerts in business as usual (BAU) or in a backlog by automatically categorising alert priority. A critical part of any prioritisation is providing the reasoning for an alert's auto-prioritisation. Alert auto-prioritisation is important because it allows investigators to focus their attention on the highest-risk probability items while relegating the lowest-risk probability items to the bottom of the priority list.

Auto-prioritisation assigns alerts a score based on likelihood to represent suspicious activity. For example, a Level 1 alert might be those that are closed (not suspicious) with little effort, Level 2 alerts are closed with some investigative effort, and Level 3 alerts are those likely to be filed as suspicious. The scoring is based on the MI model analysis using combinations of historical alert dispositions, related typologies, derived investigative triggers and bank-specific risk inputs.

For example, a Level 3 group might consist of alerts involving newer accounts, using specific fund corridors, the presence of keywords, a time-specific payment pattern, while also alerting on two high-value traditional rules/scenarios. This goes well beyond typical rule-based scoring because it evaluates multiple investigative triggers.

Once the prioritisation framework is established, alerts can then be grouped based on the concept of similarity to the identified alert profiles. As part of the process, alert group assignments would require back testing to validate the categorisations, and groups can be updated and refreshed as needed.

By using this approach, a bank learns where to focus its efforts. This results in increased efficiency and effectiveness.

## Typology development

Most rules and scenarios are developed either using out-of-the-box templates from vendor transaction monitoring platforms, or based on published regulatory red flags. The challenge when identifying new valuable behavioural typologies for investigation or rule design is searching for specific characteristics among trillions of potential data combinations. MI can help do whiteboarding for you, identifying patterns, key elements and data combinations with investigative value.

While input from AML subject matter experts can guide the process, MI can help identify behavioural patterns that don't fit any existing known rules to find 'unknown unknowns'. Identified patterns are highlighted and ranked to identify the probability of occurrence of the anomalies.

For example, two similar cash intensive businesses might both be screened by a traditional 'large cash deposit' rule. If both have the same aggregate level of transaction value, they will typically have the same alerting pattern for a standard threshold. MI can identify additional data points to distinguish the entities for rule improvement. In this example, one entity may have fewer total customers, multiple round-dollar transactions, and very few expected business-related expenses in its debit history. These characteristics are, by definition, anomalous and worthy of investigation. In this case, a new rule could be created that looks for the presence of these additional identified characteristics. Without MI, a compliance team must search for these exact characteristics among all the various potential combinations within the data.

Enhanced typology development through MI is another way to get the most out of the transaction monitoring system while minimising costly, lengthy or complex system changes.

## Conclusion

The continuing development of MI will allow institutions to implement the risk-based approach demanded by regulators while enhancing human intervention and increasing the effectiveness of transaction monitoring programmes.

Navigant Consulting Inc. has partnered with machine intelligence software company Ayasdi to offer a comprehensive solution. **Alma Angotti**, an AML consulting expert, is a managing director and co-lead of the global investigations and compliance practice at Navigant. **Timothy Mueller** is a managing director in the financial services practice, while **Joe Campbell** is a director in the global investigations and compliance practice.