Market Abuse Surveillance TechSprint (July 2024) video Transcript.

Team 1. Features Analytics

Delegate 1

Hello everyone. I'm Christina Soviani, Co Founder and CEO of Features Analytics and together with my colleagues Marco Carnini and Roswani Corespoon, we are delighted to present the TRACE surveillance platform that we developed for market abuse detection and also some of the results of the TechSprint that we executed with the FCAI. This is the next generation trace surveillance platform which is based on our proprietary 0 parameter building blocks technology and our fundamental thesis is that when you commit a crime, you leave traces behind and your job as an investigator is to go and find and monitor these traces.

However, most of the times you are not able to find all these traces, not always because the behaviour of the criminals is changing continuously. But when you find all these traces and you aggregate them together, you will constitute the the trail of the crime. And we call this trail the shape of the crime and the traces of evidence are the building blocks. So at I this we actually have built the building blocks of the crime and the he platform is continuously monitoring via these building blocks. The trader behaviour and the market activity and all the alerts that are triggered by the platform are fully explainable.

There is no parameter management and because of this new approach, in fact by at for looking for the shape of the crime, we can detect not only the known cases of market abuse, but also the below the line cases and the new emerging patterns which are a big concern for regulators. And the solution can be deployed across any region and asset class.

So I just consist of a detection engine and another management module. And the detection engine is ingesting client and market data and via the library of building blocks is continuously monitoring the trading activity. And it might happen that in certain time intervals which are detected automatically, a trader behaviour might activate a specific set of building blocks. And if the activated sets corresponds to one of the pre configure scenarios, a case is triggered as an alert for investigation and the alert management is connected and equipped with all the necessary tools. And because of our unique approach of monitoring all the activity via the building blocks and looking for this traces of evidence,

the platform can automatically optimise the current configuration of scenarios with respect to their mapping to the building blocks but also detect the below the line cases.

And in a similar way the platform can detect the emerging patterns of abuse. And additionally, the platform is coming with a sandbox via which the users can easily design new types of alerts and get instant results on the platform. Because everything is pre computed, all the building blocks and historical data.

So I this is monitoring for all the required scenarios by the regulatory bodies and it delivers effective solutions which are reducing the number of false positives with more than 80% while making sure that we detect all the manipulations. All alerts are fully explainable.

There is no parameter management, contrary to parameter based systems where we all know that you need to manage thousands of parameters and you need to continuously optimise them. In this text print we added to the IDs platform a machine learning feedback loop which is taking as an input the surveillance team decision on an alert and the alert context information. And it's training a machine learning model which is outputting confidence interval scoring, prioritising alerts in highly relevant medium and low risk categories.

As a methodology, we use several phases in the development like data labelling, model, training on different data sets and different data ranges. We tested several machine learning algorithms to make sure that not only the alerts are fully explainable but also the scoring of the alerts. And we tested and validated the alert relevant scoring as results, we obtained model temporal stability and an outstanding area under the Roc curve of 0.93. And I by design is triggering high quality alerts finding the true positives. But with the addition of this tool, we can now prioritise alerts.

And because the models are trained automatically on on your on your system, taking into account the surveillance officer decision, the model can be trained according to your risk appetite. And as a side benefit.

In fact, the model is outputting the most relevant fields from the alert context information together with our optimal values. And you can use this information in order to optimise your current parameter based systems. In case you are running in parallel parameter based systems. We don't have time for a full demo, but we prepare today a short demo showing some elements of this machine learning feedback loop.

Delegate 2

This is the either system dashboard where you can see alerts and case statistics. Now let's go to the case overview screen where we can see the list of cases assigned to the analyst who is currently logged in. Part of the machine learning loop feedback loop added in this text print is the relevance column.

Let's pick the first case and see why it was scored as high relevance. In the screen we can manage the case.

We can see attachments, comments, conclusions and more. We can see the auditor at the bottom and on the left hand side we can see insights about what the account was doing in the past six months. Now let's pick the alert, which is a spoofing type alert scored as higher relevance.

The alert is accompanied by a narrative which explains in plain English what is happening, and you can also find the alerts context information right there. Now let's go to the case to check how the alert was decided as relevant. So here we can see a few fields that are of particular importance for the analyst.

For example, the presence ratio is judged by the tool as an important field and in this alerts the ratio has a value of 10 or 77 and the depth of the 1st order on the unintended side which has a value of two is also judged as an important fields. Now let's go to the chart and validate this so we can see the account is present on both sides of the book. The bid sides in blue, which ends up trading and becomes the intended sides and the outside which is the unintended side.

When we click on the second enter message, we can see the account entered on the second level of the book in the book repair on the right hand sides. And we can also see that the ratio between the presence on the bit versus the ask is about 10 times larger, so 10.77 to be exact, as was stated before.

Delegate 1

So we want to thank FCA for this amazing opportunity and giving us access to the data, the entire FCA team, also the mentors and also all the participants today.