A 1LoD publication

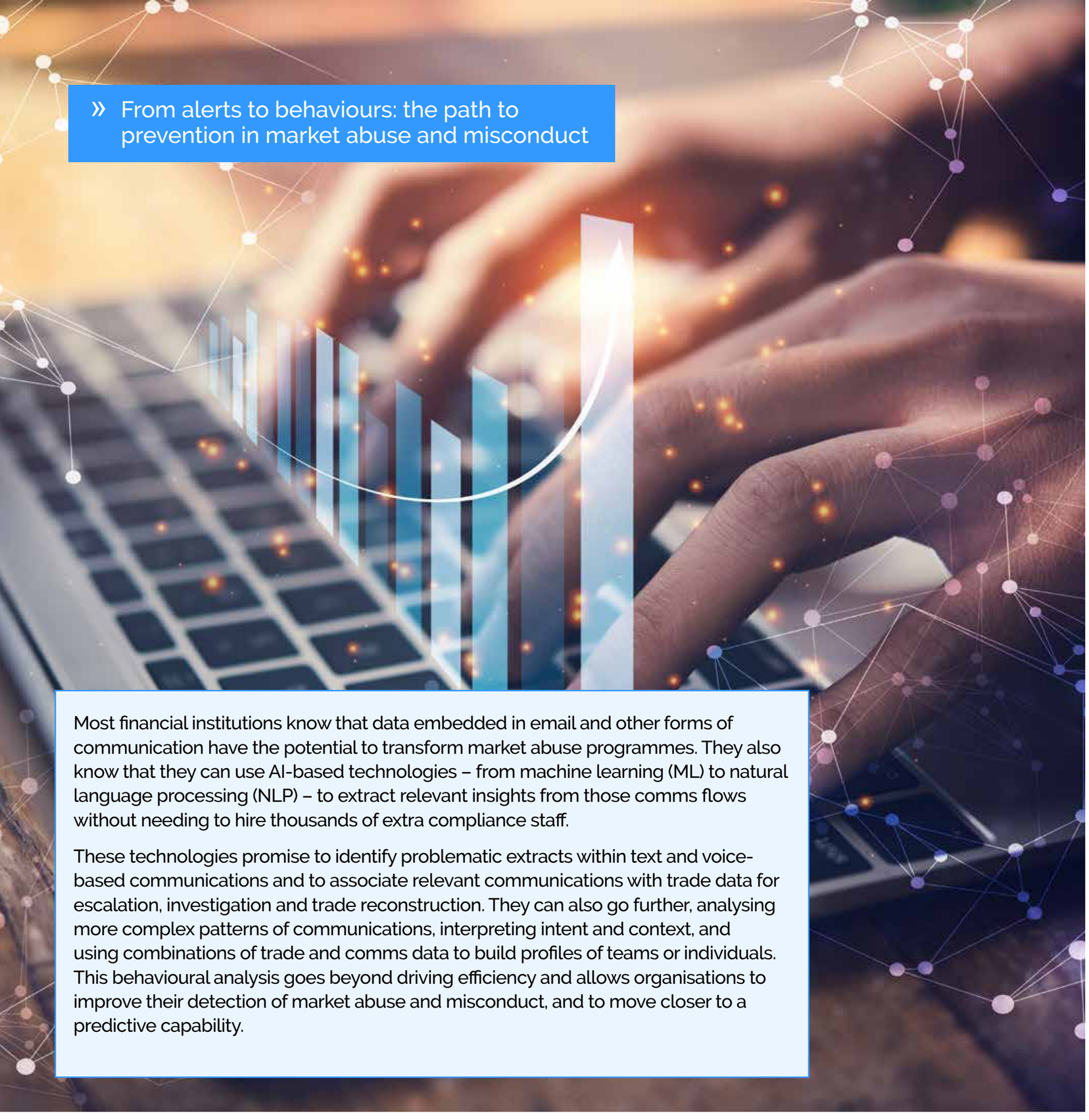
in-Focus® Report

Commissioned by: NICE · ACTIMIZE

From alerts to behaviours:

the path to prevention in market abuse and misconduct

January 2022



» From alerts to behaviours: the path to prevention in market abuse and misconduct

Most financial institutions know that data embedded in email and other forms of communication have the potential to transform market abuse programmes. They also know that they can use AI-based technologies – from machine learning (ML) to natural language processing (NLP) – to extract relevant insights from those comms flows without needing to hire thousands of extra compliance staff.

These technologies promise to identify problematic extracts within text and voice-based communications and to associate relevant communications with trade data for escalation, investigation and trade reconstruction. They can also go further, analysing more complex patterns of communications, interpreting intent and context, and using combinations of trade and comms data to build profiles of teams or individuals. This behavioural analysis goes beyond driving efficiency and allows organisations to improve their detection of market abuse and misconduct, and to move closer to a predictive capability.

Defining behaviour

That said, most banks are only just embarking on this quest and they are taking different paths to achieve these benefits. At the heart of these differences is the question, "What do you mean by behaviour?".

For one surveillance head, "it's just an anomalous data pattern – a deviation from any norm; it can be P&L data, it can be message traffic, it can be phone call patterns." In this case, in addition to using rules-based models tailored to specific markets or instruments, a more generalised AI pattern-recognition engine runs over those data types and detects anomalies that can be flagged for investigation in conjunction with any supporting trade data and actual comms content. In this definition of behavioural analysis, the anomalies create their own alerts which then need to be reviewed and investigated like any other. They create an alert stream in addition to the alerts coming from existing trade and comms surveillance processes and so contribute to the traditional problems of alert fatigue and false positives.

In this model, the behavioural approach differs from existing trade and e-comms alert generation in that it is not triggered by a single, current instance of some activity. Instead, it is a path-dependent lookback at a series of data points and is triggered when data points fall outside that trend. This data does not have to be traditional trade or comms data. Banks are creating heatmaps based on an increasing number of variables. Desks that generate large numbers of escalations (or none at all) can be flagged for further investigation, for example.

Another way of thinking about the behavioural approach is to use behaviours as substitutes for, or additions to, rules. Here, existing rules-based alerts are redefined using a behavioural approach. "For example, we are defining the key features of spoofing in terms of statistical behaviours examined over a longer period of time than simply the immediate trade data that might traditionally have triggered the rules-based alert," says another surveillance chief.

Again, the initial objective is to create an alert for existing types of market abuse or misconduct. As this surveillance chief explains: "We've effectively decided that the alert is the basic unit of surveillance, and we want to generate something that is akin to an alert, albeit the alert may have a slightly different character from what we are used to. But thinking in terms of alerts means that we have repeatability and we avoid the complications of having more generalised behavioural indicators – one of which is how to integrate that kind of behavioural analysis into existing workflows."

This is a key point. These models of behavioural analytics are reasonably straightforward to integrate into what are often still trade and comms silos. Indeed, with the right solution, they can be the beginning of holistic /contextual models that break down those silos.

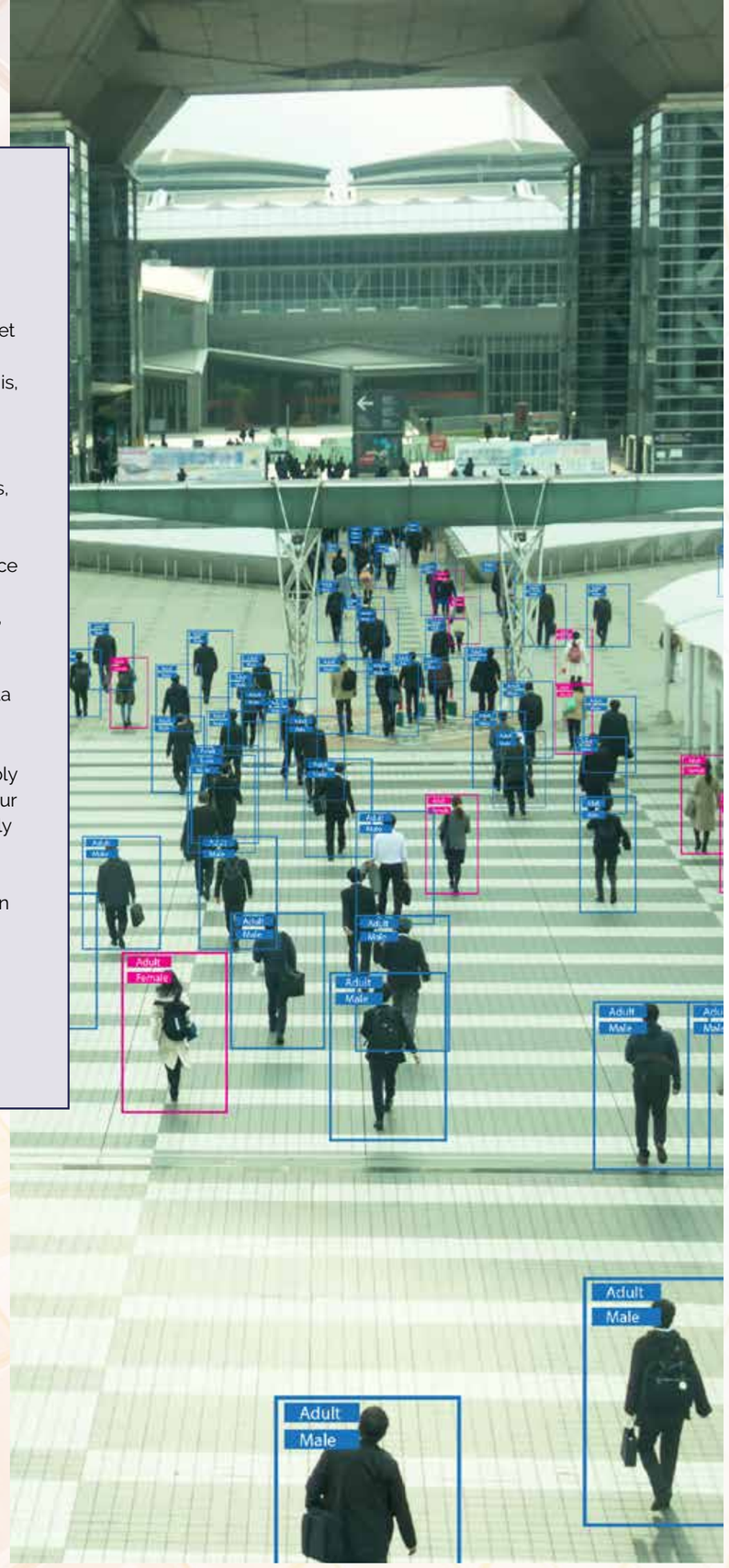
So, for example, NICE Actimize has a Holistic Behavioural Analytics solution that can be used in conjunction with the firm's Markets Surveillance solution both to reveal previously hidden risks, using anomaly detection, and to help firms more accurately assess alerts for known threats such as insider trading, spoofing and marking the close. Firms using both solutions can view alerts generated by both traditional analytics and the behavioural data associated with them within NICE Actimize's case management, so that analysts are more accurate and efficient at assessing the severity of alerts.

Intelligent alerting

This idea of behaviour-triggered alerts also extends to another type of analysis, defined as behavioural by many: in much the same way that anomaly detection engines can supplant rules-based definitions of market abuse or misconduct, so smart NLP solutions can substitute understanding for traditional lexicons. That is, they can analyse text not simply for keywords, but for context and meaning.

"Using a behavioural analytics approach to e-comms, we can reveal issues such as trader secrecy, taking advantage, intent and unacceptable styles of interaction – things like that," explains one surveillance head. These technologies can be used to enhance traditional rules-based surveillance and compliance, by identifying potential misconduct that might otherwise have been missed by sampling or human analysts because of the sheer volume of comms data flowing through institutions.

This contextual analysis, although it still fits comfortably into an alert-driven view of the world, reveals behaviour in a different sense to anomaly detection: it can literally identify and flag certain human behaviours which correlate with undesirable (or desirable) actions or cultures. For some banks, this is what they mean when they refer to behavioural analytics. And it is from this idea of being able to build up a picture of individuals or entities through how they communicate – as well as what they communicate – that leads to the most ambitious and controversial definition of behavioural analysis: risk profiling.



Using a behavioural analytics approach to e-comms, we can reveal issues such as trader secrecy, taking advantage, intent and unacceptable styles of interaction – things like that,

The trader as the entity of surveillance

Accuracy is still a potential problem with any alert-driven model. Surveillance teams are already swamped with false positives; simply adding more alert streams is not the solution. "Of course, you still have to have good data," says one head of surveillance strategy. "And even then you get false positives when you go down this road. So, in a way we have very similar problems when we try to solve that core surveillance problem with these newer approaches."

Suppliers of new behavioural technologies respond to that in two ways. First, they point out that by replacing static rules- and lexicon-based systems, they reduce the false positive rates caused by inadequate, older methodologies. (That of course pre-supposes that they work as claimed, and also that the regulators allow full replacement.)

They also argue that these new technologies are not simply additional alert engines that treat all alerts as equal (which is the root cause of alert overload). For these suppliers, and also for the leading banks, the key is risk-based prioritisation and it is here that behavioural models offer a genuine path to reducing the resources currently committed to the unsustainable (and ineffective) alert factory model.

What does this mean? The real power of the behavioural approach is to move beyond the traditional, event-driven, alert-based model to viewing the individual trader, client or counterparty as the main entity of surveillance. In this model, intelligent systems ingest data from a far wider range of data sources than traditionally associated with trade or comms alerting in order to identify high-risk individuals and entities and, potentially, to assign a risk profile to them.

To do this, banks combine trade and communications data, badge swipe data, HR data, P&L data and so on, and use pattern-recognition and other AI-based techniques to build a variety of different indicators of risk. One set of technologies looks at how individuals and groups within institutions interact and tracks the changes in those trends, for example.

As one bank describes it: "We have a graphing tool that we built in-house that looks at that relationship piece. It was somewhat derailed by work from home, but we were ingesting more and more data into it to get indications of the strength of the relationship between different individuals."

But the most significant endgame is the creation of risk profiles for individual traders based as much on behavioural data as on their appearance in alerts. Equipped with these profiles, banks can potentially solve two of the knottiest problems in market abuse surveillance and compliance.

First, they can direct resources to the riskiest places and conversely pull resources away from the surveillance of places where there is little risk. Second, they can use their knowledge of risky behaviour by individuals to start to predict where problems might arise before they do. This would represent a step-change in the operation of surveillance and compliance – and it requires a change in mindset from the regulators, from internal audit (who many bankers view as more of an obstacle to change than the regulators themselves) and in areas such as HR and privacy, where there are concerns about the legality and ethics of profiling, especially in Europe.

But the most significant endgame is the creation of risk profiles for individual traders based as much on behavioural data as on their appearance in alerts. Equipped with these profiles, banks can potentially solve two of the knottiest problems in market abuse surveillance and compliance.

The role of new technology

Those concerns aside, does profiling actually need new behavioural analytics technology? Why can't it emerge from traditional trade / comms alerts and escalations and the simpler behavioural alerts mentioned above?

One former head of surveillance at a Tier 1 global bank explains why they believe that only new technology can deliver: "Getting to the point where we can think of individuals in terms of risk is indeed the journey we want to go on. But if you rely on pulling everything you've got at the moment together for cross-correlation, you will drown. So, you have to take a preliminary step which is that you've got to start not treating all employees as equal risk. You can't take just all of your trade and comms alerts, and other behavioural data, and fold those together and expect risk-profiles to emerge from that data. You need to deploy (hopefully integrated) systems that are pushing only the higher-risk trades, the higher-risk comms and other data to surveillance officers. And to do that you need the technology that can identify risky behaviours up front."

It's the risky alerts, and other risky behaviours, such as secrecy, collusion or even bad language and harassment, that have predictive value, and to isolate those, the new AI / NLP / ML technologies are critical.

Getting easier

And that has been the issue. The challenge for organisations in making any progress towards a behavioural approach has traditionally been twofold: first, they need to be able to run their business as usual (BAU) processes at the same time as implementing and calibrating new systems and processes; second, they need these new technologies to be available as practical tools for today's surveillance and compliance use cases, not simply as interesting pieces of code operating in sandboxes. Both these challenges can now be solved at scale with off-the-shelf, enterprise-grade software.

NLP and AI models have evolved steadily over the past several years and are now genuinely able to produce meaningful insights. In particular, behavioural modelling is now a service that can be overlaid onto existing BAU processes, and existing rules-based, reactive surveillance, without disruption. Additional communications data can be ingested into essentially off-the-shelf models, mapped to existing regulatory requirements, to build, for example, employee risk profiles that then allow organisations to think predictively about conduct risk as well as to uncover previously undetected risks.

A third issue, in the past, was that banks were hobbled by the complexity and heterogeneity of the data required for these models to work. This problem is being overcome. New platforms are able to ingest structured and unstructured data, to integrate different data streams and to connect with the many venues and communications channels used by banks via APIs in order to solve the data problem.

As Steve LoGalbo, Director of Product Management for the NICE Actimize Financial Markets Compliance division, explains: "The technology is now available off-the-shelf that allows you to get access to unstructured source information, like communications data, analyse it in different ways and then take that communications analytics and collapse it into a compliance data set. In other words, you can create structured information from unstructured, and turn that unstructured data into useful business data. You can then use it to investigate a trade alert or to surface a risk that would have previously remained hidden."

Hear from Steve LoGalbo as to how and why surveillance is changing, and how surveillance and compliance professionals in the financial world (and increasingly in the non-financial world) can keep up.

About SURVEIL-X:

NICE Actimize's SURVEIL-X Holistic Conduct Surveillance offers unparalleled risk coverage for online brokers, buy-side and sell-side firms, insurance companies, crypto exchanges, regulators and more by enabling accurate detection and rapid, thorough investigation of market abuse, inappropriate sales practices, conduct risk and otherwise undetectable compliance risks to insulate firms from fines and reputational damage.

For more information check out our product brochure: Predictive, Proactive, Proven Surveillance for Rogue Trading

Or if you'd like to schedule a call or demo, please reach out: Get in touch

NICE · ACTIMIZE