

REPRINT

R&C risk & compliance

TECHNOLOGY AND AI IN CAPITAL MARKETS TRADE SURVEILLANCE

REPRINTED FROM:
RISK & COMPLIANCE MAGAZINE
JAN-MAR 2020 ISSUE



www.riskandcompliancemagazine.com

Visit the website to request
a free copy of the full e-magazine



MINI-ROUNDTABLE

TECHNOLOGY AND AI IN CAPITAL MARKETS TRADE SURVEILLANCE



PANEL EXPERTS**Paul Fagone**

Lead Partner – Regulatory Risk and
Compliance, Capital Markets
KPMG
T: +1 (212) 872 2988
E: paulfagone@kpmg.com

Paul Fagone is the lead partner in KPMG’s regulatory risk and compliance practice for capital markets. He has over 25 years of experience in the risk analytics and operational risk space. His focus is on the design and deployment of advanced analytics in the electronic trading space and has worked with his clients to build machine learning (ML)-enabled surveillance infrastructure and architecture.

**Shailesh Jain**

Director
KPMG
T: +1 (212) 954 7784
E: shaileshjain@kpmg.com

Shailesh Jain is a director in the financial services regulatory & compliance risk practice at KPMG, with over 15 years of advisory consulting experience. His focus is helping capital markets firms adapt to changes in business and technology by implementing effective control and supervision frameworks from initial vision and strategy design through execution. He is a senior leader with an extensive background in data engineering and data science.

R&C: What are the common challenges capital markets firms face with respect to trade surveillance? Historically, how have they tried to address those challenges?

Fagone: Heightened regulatory expectations and focus, coupled with an increasingly complex operating environment that includes, for example, multi-leg orders with various counterparties across multiple product types or exchanges, increasingly strain the capabilities of surveillance programmes. A couple of the common challenges we see are high alert volumes and data disconnects. In terms of high alert volumes, rules-based surveillance patterns tend to generate an unmanageable volume of alerts that require manual follow up and disposition. This white noise can not only make it very difficult to properly flag suspicious trading activity, but can also mask emerging threats. Firms should make use of advanced machine learning (ML) techniques to tune and optimise parameters and establish thresholds and move away from rule-based surveillances. As for data disconnects, data quality and availability challenges dramatically impact the integrity of trade surveillances and the corresponding volume and integrity of the resulting alerts. Disconnects between expectations and data reality can lead to a false sense of security and significant, unknown surveillance

gaps. Firms should develop and implement a data governance framework to help monitor the data quality, including establishing data sources, lineage, controls and change management protocols.

“Alert remediation is a resource-intensive manual exercise and firms struggle to keep up with the avalanche of alerts created by multiple, overlapping surveillance patterns.”

*Shailesh Jain,
KPMG*

R&C: How are firms leveraging artificial intelligence (AI) and machine learning (ML) techniques to address some of those challenges?

Fagone: Firms are starting to employ ML-enabled analytic techniques to the surveillance challenge. Specifically, we are seeing traction with respect to the tuning and optimisation process. Firms are leveraging natural language processing (NLP) to classify historical alerts, performing topic modelling on free-form analyst alert disposition text. They are then classifying

historical alerts in order to profile what a high quality alert looks like. From there, ML models are deployed to tune and optimise surveillance parameters in order to maximise surveillance yield with the ultimate objective of increasing the overall quality of the surveillance alert pool and minimising false positives.

R&C: How has the use of AI and ML techniques impacted the surveillance alert remediation workflow?

Jain: Alert remediation is a resource-intensive manual exercise and firms struggle to keep up with the avalanche of alerts created by multiple, overlapping surveillance patterns. From a workflow perspective, we have seen firms achieve significant lift by leveraging ML tools to triage and risk score live alerts. Alerts that most closely resemble the fact patterns behind certain manipulative behaviours – for example spoofing or layering – receive a higher risk score and are forced to the top of the queue. Alerts where the underlying fact pattern and data supports classification as a false positive can be tagged as such. The fact pattern can then be factored into future tuning efforts.

R&C: How have the regulators and internal risk management professionals responded to the use of ML?

Fagone: The use of ML tools and techniques, particularly the use of deep learning models, presents a unique challenge, particularly around the interpretability of the models themselves. Trade-offs between performance and interpretability must be clearly documented and understood, and we

“Globally, regulators and risk management professionals are stressing the importance of interpretability and looking to the business to clearly demonstrate that they understand the trade-offs involved.”

*Paul Fagone,
KPMG*

have seen cases where model risk management, as a discipline, has pushed for the adoption of more explainable models, including cases where error rates are higher. Globally, regulators and risk management professionals are stressing the importance of interpretability and looking to the business to clearly demonstrate that they understand the trade-offs involved.

R&C: From a trade surveillance perspective, where do you see the biggest

opportunities for improvement in terms of tools and technology?

Jain: From a tools and technology perspective, we are seeing firms converge on a number of discrete vendor platforms to manage both alert generation and workflow. With that said, we are also seeing firms augment those vendor capabilities with bespoke surveillance patterns, generally written in-house, to try and fill out the perceived gaps. We have been heavily involved with our clients trying to bridge those vendor and bespoke platforms and see the greatest opportunities in reconciling the overlap that invariably gets created. Multiple alerts from competing surveillance patterns generated on vendor and in-house solutions on the same trade population exacerbates an already intensive remediation process. Finding ways to cull the duplication is essential, and a big part of successfully integrating solutions.

R&C: Are you starting to see a convergence between surveillance platforms, such as trade, voice and e-comms? How is the use of ML techniques facilitating that convergence?

Jain: We absolutely believe the convergence of voice, communications and trade surveillances will increase the integrity of the overall trade surveillance framework and have been working with our clients

to effect that convergence. With that said, there are significant challenges to overcome, including poor recording and transcription quality, the use of slang and jargon, and the sheer volume and noise in the system. Our early research suggests, however, that the deployment of both supervised and unsupervised matching learning techniques can significantly aid the matching process – for example trade to comms – and pay dividends in terms of a higher quality alert pool.

R&C: Looking ahead, where do you see firms investing in terms of bolstering the integrity of their overall surveillance architecture?

Fagone: Across our client base, we see a number of common priorities with respect to ongoing investments. Some of those areas we have touched on, namely the use and application of ML tools and techniques to tune and optimise surveillance patterns and risk score resulting alerts. Other investments are more focused on the blocking and tackling issues associated with surveillance pattern overlap and poor data quality. Portfolio rationalisation and the decommissioning of overlapping or ineffective surveillance patterns can pay dividends in terms of managing the alert flow. In addition, investments in data quality controls at key points in the stack can not only help to ensure adequate surveillance coverage but highlight when poor data quality disrupts the surveillance platform. **RC**