

RETHINKING TRADE SURVEILLANCE

Part Two: The influence of
exchange rules on trade
surveillance and the reliance
on ballooning market abuse
taxonomies

RETHINKING TRADE SURVEILLANCE

Part Two: The influence of exchange rules on trade surveillance and the reliance on ballooning market abuse taxonomies

In Part One of this series, we looked at the operation of trading desks and the primary market abuse legislation to inform the features a trade surveillance system would need in order to be both effective and to meet regulatory requirements. We found that:

1. Global primary legislation defines market abuse from the high-level perspective of defrauding others and creating an artificiality in supply and demand and/or the price of a financial instrument.
2. The primary legislation (particularly in the USA) has been intentionally drafted to be as broad as possible, avoiding specific examples, so that it does not need to be constantly updated and will catch novel methods of market abuse without legislative changes.
3. Global primary legislation explicitly prohibits only a small number of specific behaviours themselves as examples that defraud or create artificiality. These include spoofing, wash trading and disseminating false information.
4. Bank traders rely on the shared risk profile of different instruments to hedge risk. Although this principle lets them hedge effectively, the principle can also be exploited for market abuse (i.e, cross-product abuse).

From these observations, we concluded it was possible to begin sketching the outlines of an effective trade surveillance system. So why are most trade surveillance solutions incapable of detecting cross-product abuse? Why do they rely on taxonomies with long lists of market abuse indicators and behaviours that generate many false positive alerts? Why do trade surveillance vendors speak in terms of correlations and correlated instruments when traders rarely do so?

The answer lies in the origins of trade surveillance with exchange rules.

Exchange rules and the origins of trade surveillance

Individual exchanges established their own rules long before any governmental or regulatory supervision. They did so in order to ensure that they were fair venues that afforded participants equal opportunities. Each exchange forbade certain behaviours and policed non-compliance. However, in the wake of financial crises like the Great Depression, governments progressively passed their own market abuse legislation.

The introduction of Dodd-Frank in the US and MAR in Europe in response to the Global Financial Crisis of 2008/9 changed the regulatory landscape. Financial institutions subsequently ramped up their in-house surveillance efforts and expanded the scope beyond equities to other asset classes (whether listed or OTC). However, while the legislation was significant in advancing surveillance, it was implemented against a backdrop of the only type of surveillance that was performed at that time: compliance with exchange rules. Crucially, this meant that they inherited the surveillance mindset of exchanges; namely a single-product, single-venue approach.

This inevitably led to the development of single-venue monitoring of single securities – for example, a single futures contract traded on the CME. In reality, this is not compatible with how we have already established traders operate day-to-day, which is fundamentally cross-product, cross-venue. This incompatibility has been baked into the heart of traditional surveillance, undermining the surveillance efforts of financial institutions for years. You can see this clearly in the resource-intensive nature of rule configuration and calibration and in the resulting flood of false positives present in the output.

Having roots in exchange rules means trade surveillance remains anchored by two attributes hindering effectiveness:

1. Design artifacts which make the detection of cross-product and cross-market abuse almost impossible.
2. A reliance on ballooning market abuse taxonomies.

Reliance on ballooning market abuse taxonomies

The majority of surveillance teams and systems rely on market abuse taxonomies to detect abuse. These are a way of categorising behaviours which act as potential signs of abuse, including terms such as advancing the bid, pump and dump, smoking and many others. They too form part of the legacy of surveillance emerging from exchange rules.

Recognising the failure of traditional (exchange rules based) approaches and with the then-available technology limited, compliance departments opted to cast a wider net. They began looking for trading patterns which might be associated with abuse rather than themselves being abusive. Unfortunately, these behaviours are very often also a by-product of normal market making and risk taking. The consequence of adopting this approach? The large abuse taxonomies we still see today and the overwhelming rates of false alerts as a result.

The fact that each abuse typology only searches for patterns which may relate to abuse rather than corresponding to it, immediately compromises accuracy. To compound matters, these taxonomies were designed with rigid rules in mind which need constant updating and recalibration. The result is a surveillance system that generates overwhelming numbers of false positives entirely by design.

As we discussed in Part One, the primary legislation and corresponding application by the courts is focused on

whether the trading activity had a market impact and whether the activity was executed with the intent (or scienter) of artificially impacting markets and creating a false or misleading appearance, with respect to the market and/or supply and demand of an instrument. The primary legislation largely and intentionally avoids defining individual abusive behaviours, nor does it provide a taxonomy of market abuse types with which surveillance systems should adhere to.

We now see the mismatch between the surveillance implied by the operations of a bank trading desk, the primary legislation and the surveillance observed today. Much of this discrepancy reflects the historical sway held by exchange rules on surveillance frameworks.

Example: Advancing the Bid

Let's take the category of 'advancing the bid' as an example of a taxonomical category which only loosely aligns with market abuse.

Importantly, advancing the bid is not defined in primary legislation but is actually solely referenced in the ESMA guidance document of February 2015. Section 2.3 (Technical Guidance) of that document includes subsection 11, which states:

"The following practices **could** relevantly clarify Indicator A(f) of Annex I of MAR..." (*emphasis added*)

Subsubsection (d) of subsection 11 then goes on to state:

"Entering orders to trade which increase the bid (or decrease the offer) for a financial instrument, related spot commodity contract, or an auctioned product based on emission allowances, in order to increase (or decrease) its price — usually known as 'advancing the bid'."

First of all, subsection 11 describes advancing the bid as a practice which "could" be a sign of market abuse, but it is clear that it is not considered abuse in itself. Secondly, nowhere in that document or elsewhere is it stated that firms must monitor for this behaviour.

Furthermore, the crucial wording here is "in order to increase (or decrease) its price". This wording implies scienter and mens rea, suggesting that intent needs to be proven. This requirement was demonstrated and further clarified in Circuit Judge Richard Sullivan's ruling against the CFTC in November 2018 (CFTC v. D. Wilson & DRW).

The dismissal ruling made it clear that the CFTC needed to prove that (1) the defendant(s) specifically intended to cause an artificial price, (2) the defendant(s) possessed the ability to influence the market price, (3) an artificial price existed and (4) the defendant(s) caused the artificial price.

The Court found that "the CFTC offered no evidence or explanation demonstrating that ... prices were artificially high." Additionally, the Court found that "the CFTC failed to prove that Defendants intended to cause artificial prices."

Financial firms' interpretation of the ESMA guidance has resulted in building controls which look for signs of a trader

moving their bid up (or offer down) repeatedly, because it could be a part of an effort to spoof or ramp the market. However, there are numerous reasons why a trader may need to engage in this behaviour for entirely permissible commercial reasons. Indeed, effective market-making requires a trader to move their bids and offers in line with the market on a continuous basis.

At what point then does such behaviour occur in an impermissible form? The behaviour will only constitute spoofing, for example, if the trader both creates market impact (via advancing the bid) **and** executes a trade on the other side of the market (i.e., advancing the bid in this context is essentially a spoof order used to force an execution). Crucially, if a trader only moves their bid in line with the market, then they are simply market making (or are just keen to have an order filled). It is the combination of creating a market impact via advancing the bid **and** executing on the other side of the market that is suspicious. Advancing a bid without an execution on the other side of the market is not a sign of anything and lacks demonstrable scienter and/or mens rea.

The behaviour that the trade surveillance framework is trying to capture here is spoofing. However, because traditional trade surveillance acts on a single security, single venue basis, it must allow for the fact that it may not capture the trade on the other side of the market as it might be in a different instrument. In an attempt to remedy this, the net has been cast widely and compliance teams look for all instances of advancing the bid regardless of whether an opposing trade exists. In theory, this permits the detection of abuse where a trader submits a spoof order in one instrument and trades in another. In reality, the result is a surveillance team so overwhelmed by false alerts created by genuine market-making activity that the true signal is drowned out by the noise.

This has a steep cost in terms of accuracy.

To recap, the historical evolution of trade surveillance from exchange rules has meant that legacy surveillance controls borrow from a framework intended for listed equities. This is particularly clear in relation to:

1. Their default 'single security, single venue' approach to surveillance which produces an inability to detect cross-product abuse.
2. Their reliance on ballooning market abuse taxonomies which are essentially the product of attempts at shoehorning other asset classes into an order flow-based surveillance model, itself originally from listed equity markets.

The Next Steps For Trade Surveillance

How should trade surveillance evolve? How can it overcome these fundamental drawbacks in its present architecture?

Three key remedies stand out:

1

Work closely with the front office

Firstly, surveillance and compliance departments need to engage deeply with the front office. Specifically, they need to increase their understanding of how the front office operates.

In Part One, we explored how a bank's trading desk makes money and how its traders view

their risk. We demonstrated that cross-product abuse is an inherent risk which was effectively ignored by traditional trade surveillance frameworks. Effective monitoring requires an understanding of front office operations and its analysis of risk.

2

Return to the primary legislation

Secondly, surveillance teams should ensure they use the primary legislation when creating risk frameworks. The primary legislation is the fundamental source of all definitions of market abuse.

In Part One, we reviewed the key primary legislation from around the world to uncover these definitions. They were generally high-level and tended to avoid explicitly defining specific behaviours that constitute market abuse, with a few exceptions. Much of the legislation can be summarised as: trading to take risk or to facilitate a customer trade is legal but trading with the sole aim of moving the price is not.

By contrast, modern taxonomies are only derived indirectly from the primary legislation. The size of these taxonomies is not a reflection of what the primary legislation explicitly

prescribes. Instead, it is a reflection of how incompatible traditional exchange-based surveillance is with how traders actually behave. These taxonomies have ballooned as they try to capture every possible type of behaviour that may be a sign of market abuse (rather than actual market abuse) even though the behaviour itself may not be linked to instances of market abuse. By returning to the primary legislation, surveillance teams consider first principles with renewed purpose.

This approach complements deeper engagement with the front office. Once surveillance teams have a complete understanding of how their trading desks operate and how the individual traders view risk, they can make an evaluation against the primary legislation and create a tailored market abuse risk control framework.

3

Re-evaluate the risk assessment process

Finally, surveillance teams should apply this knowledge to their risk assessment process. We have explored how some market abuse categories, such as 'advancing the bid', are merely looking for indicators of market abuse. As we have argued, this stems from the contradiction embedded within exchange-based surveillance tools.

To overcome this, surveillance teams must evolve the thinking which presently informs their risk assessments. Specifically, they should use their understanding of how the primary legislation applies to their trading desks to

reconceive their own internal market abuse taxonomies and control frameworks. In doing so, they would create risk taxonomies that targeted true market abuse.

Such a control framework would dispose of controls and alert types which merely look for indicators of market abuse. The benefits of this approach for surveillance teams cannot be understated. One: a significant reduction in the number of false positives would save both time and effort. Two: once the noise from false positives dissipates, true instances of abuse become far easier to detect.

Advance your surveillance function

Improve your detection of market abuse, uncover cross-product abuse, and prioritise high-risk alerts.

Reach out to learn more.



tradinghub.com/MAST



tradesurveillance@tradinghub.com



Legal Disclaimer

Copyright © 2024 TradingHub Group Limited, a private limited company registered in England under company registration number 07382307 and registered address at 21st Floor, Broadgate Tower, 20 Primrose Street, London EC2A 2EW. TradingHub Group Limited, and if applicable, a TradingHub group company (together "TradingHub"), are providing this document to the addressee("Addressee") under the following strict conditions:

This document contains confidential information and is intended solely for the Addressee. You will be an Addressee if you have received this document from TradingHub (or your receipt of it has been approved by TradingHub).

If you are not the Addressee or you have otherwise received this email in error, please notify us by contacting legal@tradinghub.com, immediately and permanently delete this document and do not use, copy or disclose the information contained in this document.

This document is being provided to you solely for information purposes. Nothing expressed or implied in this document is intended to create legal relations between TradingHub and an Addressee (or any third party).

TradingHub is the owner or the licensee of all intellectual property rights in this document. Those rights are protected by copyright laws and treaties around the world. All such rights are reserved.

You are not permitted to directly or indirectly (including any attempt to) reverse engineer or decompile anything contained in this document, any part thereof or any information contained therein.

You are not permitted to share this document with any other person, without prior written permission from TradingHub (by email shall suffice).

This document is being provided to you on an "as is" basis. TradingHub (and its third party licensors) do not make any representations, warranties or guarantees, whether expressed or implied, as to the accuracy, completeness or timeliness of this document (or any part thereof), or as to any results obtained or inferred by an Addressee or any third party, and shall not in anyway be liable to an Addressee or any third party for any inaccuracies, errors or omissions herein.

TradingHub (and its third party licensors) do not have an obligation to update, modify or amend this document or to otherwise notify an Addressee or any third party in the event that any matter stated herein, or any opinion, projection, forecast or estimate set forth herein, changes or subsequently becomes inaccurate.

TradingHub (and its third party licensors) do not have any liability whatsoever to an Addressee or any third party, whether in contract (including under an indemnity), in tort (including negligence), under a warranty, under statute or otherwise, even if foreseeable, in respect of any loss or damage suffered by it as a result of or in connection with: (a) any opinions, recommendations, forecasts, judgements, or any other conclusions, or any course of action determined, by it (or any third party), whether or not based on this document; or (b) use of or reliance on this document.