Mitigating Market Abuse

Lorne Chambers, Head of Sales and Account Management for SMARTS Integrity, NASDAQ OMX, looks at the challenges faced by regulators and how they can bridge the gaps in cross-market surveillance.
The responsibility of cross-market surveillance, which has traditionally been levied on exchanges, is rapidly expanding to encompass industry regulators as part of a collective effort to mitigate market abuse. Following the implementation of new regulatory policies in 2007, particularly Reg NMS in the US and MiFID in Europe, enhanced competition and market fragmentation have been key elements in exposing gaps in surveillance coverage across trading venues.

Current market structure has increased the potential for abuse; indeed, practices such as front-running, spoofing, and insider-trading can now be spread across multiple venues by market participants in an effort to reduce the chances of detection. For example, a participant might layer the order book on one venue and then proceed to trade on another venue in the same instrument.

Already facing increased competition and cost pressures, there are compelling reasons for firms to consolidate surveillance within regulators or third parties such as the Investment Industry Regulatory Organization of Canada (IIROC) and the Financial Industry Regulatory Authority (FINRA) in the US. These organizations and regulators can potentially achieve economies of scale and monitor multiple venues in a coordinated manner.

This regulatory shift is occurring primarily across markets in Europe and North America. Europe faces a unique challenge in establishing a surveillance program that offers a consolidated view of data because it must navigate the local rules and regulatory bodies of over twenty member nations. As one of many efforts to remedy this situation, the European Securities and Markets Authority (ESMA) was formed in January 2011 with the purpose of harmonizing approaches across Europe through its guidelines on MiFID. However, unlike IIROC, which oversees market surveillance in Canada, ESMA currently does not have the capability to execute and monitor a pan-European surveillance program.

In addition to ESMA, the Intermarket Surveillance Group functions as a member-based organization bringing together over fifty exchanges, market centers and market regulators across the world to coordinate surveillance policies and minimize cross-border manipulation. The International Organization of Securities Commissions (IOSCO) and the Basel Committee on Banking recently fronted another initiative with the joint publication of a new set of standards preventing firms from capitalizing on rule-based differences between nations and improving transparency within derivatives markets.

With the exception of Australia, which recently employed a comprehensive surveillance program through the Australian Securities and Investments Commission (ASIC) to regulate the Australian Securities Exchange and Chi-X, the issue of cross-market surveillance is not playing out to the same degree in the Asia-Pacific region as it is in the US, Europe and Canada. There is however potential for South America to face this issue in the near future, especially in Brazil where there is heightened public interest in establishing a new trading venue.

**Why Regulators?**

In the face of this complex multi-venue landscape, regulators offer an enhanced level of confidentiality in cross-market surveillance that is challenging to achieve at the broker-dealer or exchange levels. There is a significant need among surveillance departments at exchanges and other trading venues to be able to share sensitive information in a secure manner without relinquishing their secrets to competitors; for example, the ability to reverse engineer trading strategies from customer identified data.

In addition, there is a growing trend to outsource to third party quasi-regulators, such as FINRA and IIROC, that maintain a degree of separation from trading activities and possess the necessary tools and budgets to handle such complex operations. The majority of Canadian trading venues utilize IIROC’s services, which offer a full-range of monitoring and regulatory programs. In addition, the New York Stock Exchange (NYSE) and the Nasdaq Stock Market outsource T+1 surveillance to the US self-regulatory organization (SRO), FINRA.

Many surveillance solutions are becoming increasingly outmoded by immense volumes of data; up to ten billion trading messages can occur per day in a given country—NASDAQ OMX alone processes more than four billion transactions daily. Shifts in liquidity among venues can also result in market share and exposure in a venue quickly changing.
Key Challenge for Regulators

Budget is generally a key challenge for regulators. Regulatory IT budgets are typically much lower than the IT budgets of the firms they monitor. Yet, regulators need the monitoring tools that will enable them to monitor the key risks associated with market abuse or other trading irregularities across multiple venues.

Key attributes regulators should look for in a surveillance solution include:

- Domain specific technology proven in multiple jurisdictions as opposed to a generic solution being applied to a specific domain.
- Capable of both real-time and next-day analysis to avoid built in obsolescence.
- Ability to monitor across multiple global venues.
- Functionality to normalize multiple sources of structured and unstructured data; in other words, flexible enough to incorporate additional data from other regions and social media.
- High capacity, providing the ability to process billions of messages per day.
- Partner with a committed provider that has invested significant time and resources into dealing with the complexities of cross-market surveillance and will remain adaptive to future technological advancements.

from minor to significant; so a market’s regulatory risk can quickly escalate to the point that systematic monitoring is essential. One of the approaches suggested in Europe holds regulators accountable for consolidating order books for listed companies that trade primarily in their country. The notion of primary market has the potential to change regularly for certain instruments in a competitive environment.

Consistency in identifying market participants and their trading activities is essential to ensuring market integrity and fostering a more unified and systematic approach to cross-market surveillance. The Consolidated Audit Trail initiative in the US mandates that SROs submit a national market plan that would lead to the creation of an audit trail, which tracks the life of an order from broker to exchange/ATS with client-identifying details. This is a major step considering most markets outside of the Middle East and some Asian countries do not systematically identify client accounts in surveillance data. There are end-user technologies that proffer solutions to such challenges, including SMARTS Integrity from NASDAQ OMX, which recreates order books from exchange data, links related instruments, and consolidates data across multiple venues to identify and combat potential market abuse.

As regulatory and surveillance needs can remain highly market-specific, there is a complimentary argument for self-monitoring within exchanges; they maintain a more detailed vantage point of both the market and their listed companies than regulators and third party organisations, allowing them more effective insight into market activity. In Europe, legislation is currently under consideration that could allow regulators to outsource consolidated market surveillance to third parties, which would include local exchanges.

Next Steps for Regulators

Establishing a manageable budget in times of austerity and attracting the right staff will be paramount if regulators are tasked with deploying successful cross-market surveillance programs. The process of normalizing multiple formats and linking data from multiple sources will be equally important as market structure and surveillance needs continue to evolve.

Those looking to find any unfair advantage and exploit markets are investing heavily in technology, so it is critical that regulators partner with industry solutions that have the resources to continue to innovate and take advantage of new technology such as big data, cloud computing, social media and sentiment analysis. Real-time cross-border systems coupled with expertise will further aid in linking a worldwide community of regulators.

In the US, the National Market System plans to implement a Consolidated Audit Trail as one of many steps in an effort to improve market compliance and regulation. Other regions, including Europe, are putting in place a framework for industry-led consolidated tape solutions and these may well learn valuable lessons from the progress being made in the US over the next several months.

One thing is abundantly clear, in the current era of market fragmentation and trading across markets and countries, it is essential for regulators to be able to monitor activities across multiple markets.