THOMSON REUTERS ACCELUS™

SPECIAL REPORT: Are U.S. regulators ahead of European counterparts in tackling tech-enabled market abuse?

Jun 22 2017 Rachel Wolcott, Regulatory Intelligence

Regulators worldwide handed out nearly $70 million in fines for technology-enabled market abuse and manipulation between 2009 and May 2017.

U.S. regulators appear to be at the forefront, having taken at least 20 enforcement actions against traders using techniques such as spoofing, wash trades and painting the tape, according to data supplied to Thomson Reuters Regulatory Intelligence by Corlytics (View PDF). By contrast, European and Asian regulators have taken about 10 enforcement actions for similar breaches.

Whether this data demonstrates superior enforcement ability on the part of U.S. regulators such as the Commodity Futures Trading Commission (CFTC), the Securities and Exchange Commission (SEC) and the Financial Industry Regulatory Authority (FINRA) is unclear.

Equally, lawyers specialising in algorithmic trading and market abuse cases have suggested that U.S. regulators' lead in terms of fines and enforcement actions may not necessarily be an indication European financial regulators are lagging behind in market abuse detection and enforcement. It may instead be a sign regulation and pre-trade risk checks aimed at preventing this kind of abuse are working better in Europe.

"One reason you are finding fewer cases involving spoofing [in the UK] at the moment is that they take time to process, with parallel market operator and regulator tracks," said Conor Foley, advisor, government and regulatory affairs at Norton Rose Fulbright in London.

Algo/high-frequency trading and market abuse: what is it?

Since the Flash Crash in 2010, algorithmic and high-frequency traders have attracted greater regulatory scrutiny aimed at preventing systemic risk and clamping down on market abuse.

There have been many big cases in the United States and some in the UK where traders have been fined and sometimes banned for spoofing, wash trades and painting the tape (View PDF for definitions). These techniques often deploy a simple algorithm to flood the market with bids or give the appearance of interest in a security. In effect, technology makes it easier for traders to execute what used to be manual market abuse.

"When you go into algorithmic and high-frequency trading there are more opportunities to cheat than in manual trading. Often those doing algo trading have managers who have no clue what they're doing. Having trading managers who don't understand what their traders are doing is a recipe for risk," said John Byrne, chief executive at Corlytics in Dublin.

Electronic anonymous markets have in some respects made it easier to commit market abuse. It has made it challenging to detect when regulators are looking at sub-second data for evidence of misconduct; however, the more frequent kinds of market abuse that are labeled as being algo or HFT-related are generally manual traders using simple technology to abuse and manipulate markets. These are the people being caught, fined and banned.

"In reality some of the biggest offenders in the United States who have been prosecuted have not been HFT or real algo traders. They're point-and-click guys with an algo back end — like the Igor Oystacher and 3Red Trading case, the Hound of Hounslow and others," said Sam Tyfield, a partner at Vedder Price in London.

Algorithmic and high-frequency trading sometimes creates the suspicion of abuse when none has occurred. It can also create mini-flash crashes only detectable by use of big data computing to pinpoint sub-second activity. Some estimates have suggested there are up to 10 sub-minute flash crashes daily.

That is not market abuse, though. Algorithmic and high-frequency trading advocates point out that these firms are expensive to set up and staff. Most firms are not setting out to spend big only to be caught and banned.

"Algos may do what amounts to spoofing, because sometimes there are feedback loops that create a spoofing pattern. That's what happens when you hear about mini-flash crashes. Most of the abusive behaviour is done by manual traders with rudimentary algos no more sophisticated than a macro in MS Word," said Michael Friedman, general counsel and chief compliance officer at Trillium, a New York-based prop trading firm.

Enforcement actions more prevalent in the United States

Since 2016 there have been a combined 12 enforcement actions on spoofing brought by the CFTC, FINRA and the SEC. The CFTC took seven of the actions in that period, demonstrating the vulnerability of the futures and commodities markets to spoofing.

One of FINRA's 2016 enforcement actions was to fine Los Angeles-based Electronic Transaction Clearing, because its "supervisory systems and procedures and risk management controls were not reasonably designed to supervise and manage the risks of its market access (MA) business …"

The firm, which catered to plenty of foreign investors, was also cited for failure "to dedicate sufficient compliance resources and staff to meet its regulatory responsibilities … to conduct adequate follow-up and review of potentially manipulative activity …"

Compare the U.S. level of enforcement action with only three Financial Conduct Authority (FCA) actions on spoofing since 2011. Those were Swift Trade, Michael Coscia and Da Vinci Invest/Mineworld.

Corltyics lacks data on enforcement actions taken by the French or German regulators. The Autorité de Marchés Financiers (AMF) website shows no enforcement action taken for spoofing and other kinds of technology-enabled market abuse.

A BaFin spokeswoman said the regulator does not categorise its market abuse statistics into spoofing, layering, wash trade and painting the tape activities. The BaFin has pressed charges in about 500 cases since 2009 due to false or misleading signals with regard to the supply of, demand for or price of a financial instrument (Article 12 (1)(a) of the MAR). She did not indicate whether any of these cases ended in fines or bans.

Research undertaken by TRRI did not reveal any enforcement action taken in the European Union similar to FINRA's Electronic Transaction Clearing case, which was for failures with regard to pre-trade checks for direct market access (DMA) providers or for a lack of compliance resources dedicated to detecting potential market abuse.

Potential reasons for the enforcement imbalance

Lawyers have pointed to a number of reasons that could explain the imbalance between U.S. and European enforcement action. Those explanations range from differences between the U.S. and European market environments to differences in regulatory approach.

European and UK futures markets tend to be less fragmented and more monopolistic than those in the United States. In theory, that makes it easier for regulators and exchanges to detect market abuse. In Europe many instruments will be traded on one exchange only: for example, Brent Crude Futures are traded only on the ICE. The argument goes that it is easier to spot manipulative trades before they hit the market, because trades are not spread among venues. That could be one reason fewer enforcement actions are seen for spoofing futures contracts in Europe.

Futures exchanges' monopolies may protect them from spoofing and other market abuse, but that does not apply to Europe's stock markets. A stock that is listed in London, for example, will trade on multiple venues and in many cases will be inter-listed on other European exchanges. That makes abuse harder to detect if traders are spoofing by putting orders through multiple venues.

"Stocks, by contrast, trade on multiple exchanges. In order to get a complete picture of what a trader is doing, you need to get the data from all those different markets. Each one of those markets is only seeing a fraction of the puzzle. You need someone to take the fractions of the puzzle from different exchanges and put them together. MiFID II and MAR create the common language and common recordkeeping requirements to make that piecing together straightforward, but it's left in the hands of each national competent authority to pick up on it," Friedman said.

So far, no cases of multi-venue spoofing, or even outright spoofing of equity markets, have been made public in Europe, if there have been any. The United States, by contrast, has seen many such cases.

Some have argued, however, that in Europe it is possible that manipulative orders in all instruments are more likely to be caught before they hit the market. In the UK and the European Union strong pre- and post-trade risk checks have been in place since 2012 and in some cases even earlier. Futures commission merchants (FCMs) or general clearing members (GCMs) often catch abusive orders before they hit the matching engine, Tyfield said. Similarly, many European exchanges are geared up to detect abusive orders before they are executed.

"The market surveillance teams on these exchanges are hot right now. The scrutiny of the teams asking member firms for reasons why certain trades were made, has increased. Nine times out of 10 there is a perfectly good reason for what's happened. Firms keep records. They make sure an audit trail is there," Tyfield said.

SEC rule 15c3-5, brought out in April 2014, was supposed to ensure there was an independent risk layer between the market participant and the market. The level of compliance to this rule is said to be low, however, and there may be more instances of failure similar to the 2016 Electronic Transaction Clearing case.

"15c3-5 had at its heart a good principle: that no one should be permitted 'naked' access to trading venues. It was ahead of the curve to a large extent and a forerunner to similar rules in the EU and, just like any regulation at the vanguard of change, was tested by market participants," Tyfield said.

Differences in regulatory approach

U.S. financial services regulators tend to be more determined in their enforcement actions and to levy many more, and higher-value, fines than any other financial services regulators globally. European regulators, on the other hand, tend to pursue cases when cooperation is offered. Some critics told TRRI that such an approach meant they might not be pursuing complex market abuse cases.

This does not mean market abuse is not happening, but experts doubt spoofing is taking place on the same scale in Europe as it is in the United States.

"Catching malefactors is not endemic [in Europe] in the way it is in the United States. That could be for any number of reasons, including that the FCM and GCM community is developing pre-trade risk management systems and undertaking due diligence on its clients, so are more likely to catch abusive orders before they leave its (or their clients') systems," Tyfield said.

While European regulators may prosecute fewer spoofing cases, it does not mean they are unable to do so.

"European regulators are in the situation where a big deal for them might be something like the 2013 Coscia case. Coscia was a seminal market abuse enforcement action. The FCA is a sophisticated regulator yet even it struggles to make cases in commodity derivatives markets. But with Coscia it achieved an unusual trifecta – market manipulation, commodity derivatives case, and high-frequency trading strategy," Foley said.

Foley said the Coscia spoofing case was a good example of the FCA's ability to handle tough cases. Concluded in 2013, the case against Michael Coscia was a challenge because it was a commodities futures case. Coscia himself had no permanent place of business and deployed a sophisticated algorithm and trading techniques to facilitate the spoofing. The FCA was able to analyse, with the cooperation of ICE, sub-second data to identify the abusive orders.

The advent of the Markets in Financial Instruments Directive II may bring about more market abuse cases. Regulators will have access to an unprecedented amount of transaction data, from which they should be able to delve more deeply into trading patterns that could indicate market abuse.

"Under MiFID II the amount of data regulators will be sitting on and have to do something with will quadruple, at least. There will be terabytes of additional data per national competent authority, per day that will have to find its way into a central repository to be analysed, so it remains to be seen what (if anything) the authorities can do with that information, particularly the information to do with orders which do not make their way onto platforms or generate transactions," Tyfield said.

European regulators have begun to bolster their analytical and market surveillance capabilities in anticipation of MiFID II. The FCA will have capabilities to test algorithms before they are deployed in the markets. Its Zen system, which collates around 20 million transactions per day, is said to be market-leading.

In France, the AMF is deploying its new system, dubbed ICY. Regulators around the world will begin to use artificial intelligence and big data techniques to up their games in market surveillance and market abuse detection.

Finally, the FCA's appointment of Vincent Coughlin QC to replace Claire Lipworth as its chief criminal counsel is widely viewed as an indication of its intent to pursue many more financial crime cases, including market abuse.

Multi-broker spoofing: an emerging risk

Multi-broker spoofing is a new trend highlighted by an SEC and Federal case against two New Jersey day traders last December.

The SEC charged Joseph Taub and Elazar Shmalo with manipulating more than 2,000 NYSE- and NASDAQ-traded stocks and reaping more than $26 million in profits from their successful trades. The SEC alleged the defendants "utilised dozens of accounts at various brokerage firms to carry out their scheme undetected, typically using two at a time to engage in a flurry of manipulative trading activity that usually lasted less than five minutes".

Friedman pointed out that while the United States and Canada were positioned to deal with multi-broker spoofing, the UK and other European jurisdictions might not be.

In the United States, he said, the long-term solution for this kind of abuse was the Consolidated Audit Trail (CAT), which will come into being in late 2019. In the meantime, detecting whether multi-broker spoofing venues are cooperating to collate their collective order flow is to be reviewed by FINRA. FINRA also has its Cross-Market Report Cards programme that permits it to alert brokers that they may have received a piece of a sliced-up spoofing pattern, Friedman said.

The Investment Industry Regulatory Organisation of Canada receives order message data from venues for centralised surveillance. Those messages already contain customer ID tags, which Friedman said made detection easier.

European Union venues are, of course, subject to the Market Abuse Regulation, which requires them to look for multi-venue spoofing, but is unlikely to solve multi-broker spoofing.

"If a trader using Broker A to place some bids on Euronext, and Broker B to place more bids on BATS, and then sells at the resulting artificially increased pricing using Broker C on Turquoise, none of the Euronext, BATS or Turquoise will have adequate data to detect this scheme, nor will any of Brokers A, B or C," Friedman wrote in a recent piece for Automated Trader.

While MAR and MiFID II require data sets to be collected, it was national competent authorities' responsibility to reassemble that data and analyse it, Friedman said. It is unclear whether European regulators' surveillance tools are geared up for multi-broker spoofing.

REMIT uncovers market abuse on EU energy markets

Outside the scope of financial services regulators, enforcement actions for spoofing and other forms of market abuse have been common in Europe's wholesale energy markets since Regulation on Wholesale Energy Market Integrity and Transparency (REMIT) transaction reporting came into force in 2015.

"If you're looking for volume of [market abuse] cases, it's not really market abuse in financial instruments that you should look at. In the power and gas markets we're seeing enforcement actions taken by OFGEM, not the FCA. OFGEM sent out a letter last year telling market participants that certain activity constitutes market manipulation as defined in REMIT," Foley said.

The REMIT Annual Report 2016 showed a steady increase in the number of new REMIT violation cases reported (page 40). In 2013 there were 12 cases and in 2014 and 2015 there were 33 cases respectively. Most of these were for market manipulation linked to insider dealing.

"In the coming years, the Agency expects further increases in the number of cases under review, supported by the surveillance activity that it has been conducting since the start of data collection," the Agency for the Cooperation of Energy Regulators (ACER) said in the annual report.

OFGEM's website does not show any open investigations specifically for market abuse.

Rachel Wolcott *is risk management and financial regulation correspondent for Thomson Reuters Regulatory Intelligence.*
