GIR
Global Investigations Review

NEWS

Spoofing: Why does UK enforcement lag behind the US?

21 May 2020

Zach Fardon, Aaron Stephens, Patrick Montgomery and Joanna Harris

King & Spalding's Zach Fardon, Aaron Stephens, Patrick Montgomery and Joanna Harris discuss the distinct legal frameworks applicable to "spoofing" cases in the US versus the UK, and why UK enforcement efforts may appear lacklustre compared to the US.

"Spoofing" is a type of market manipulation affecting financial markets across the world. The ability to spoof largely arises from, and is exacerbated by, electronic markets and technology-enhanced trading tools. However, two of the world's most important markets have adopted noticeably different postures to enforcement in this area. The US and UK legal frameworks are also very different, with the US focusing on the intent of a spoofing trader, while the UK focuses less on intent and more on the market effects of spoofing-like conduct. In many respects, the UK legal framework should provide a more straightforward route to punish spoofing traders – but the US has been the more aggressive enforcer to date.

Aggressive, but not always successful (at least on the criminal front). In recent years multiple criminal and regulatory authorities – including the Department of Justice (DOJ), Commodity Futures Trading Commission (CFTC) and the Securities and Exchange Commission (SEC) – have sought to identify and punish spoofing traders and their firms. Only one criminal trial has resulted in a guilty verdict (*US v Coscia*), with two trials resulting in an acquittal and a mistrial, respectively. More recently, however, the DOJ has obtained guilty pleas and cooperation from individuals and has indicted a number of traders who await trial. Regulatory sanctions have been imposed on various individuals and firms and putative class actions have been filed in New York and Chicago.

In the UK, the Financial Conduct Authority (FCA) has issued final notices against individuals (notably Michael Coscia in 2013 and Paul Walter in 2017) and obtained

First published on the *Global Investigations Review* website, 21 May 2020.

High Court remedies against Swift Trade in 2013 and Da Vinci Invest and Mineworld in 2015. Since 2017, however, there have been no public regulatory outcomes, and no UK authority has pursued a criminal prosecution related to spoofing. In response to a freedom of information request filed by GIR, the FCA confirmed that it did not open any new spoofing investigations in 2019 and only opened one the year before. There are five ongoing FCA investigations into spoofing, four relating to individuals and one concerning a company.

The infrequency of such actions (especially in comparison to US efforts – see *US enforcement of spoofing* below) is notable given London's prominence in the global financial markets *and* the powerful anti-spoofing laws in the UK's toolkit. Below we provide a brief comparative overview of the relevant legal/regulatory frameworks in the US and UK and our thoughts on why this apparent disparity in enforcement exists.

What is spoofing?

It may take various forms, but typically involves a trader submitting, and then cancelling, offers or bids in a security or commodity with no intent to execute those orders when placed. A spoofing trader's goal may be to alter the appearance of supply or demand (as reflected on an electronic exchange or trading platform) and thus move the price of an instrument on one side of the order book, thereby "spoofing" other market participants into transacting with him on the other side of the order book. The victims of spoofing are sophisticated human (or algorithmic) trading counterparts and market participants, not customers, clients or others to whom the trader may owe a fiduciary duty.

A spoofing trader may utilise high-frequency trading technology (eg, to flood a market with fake orders and cancellations, all within milliseconds), but manual traders may also engage in spoofing-like conduct. Indeed, much enforcement activity to date has involved manual traders who are alleged to have engaged in spoofing to trick an algorithm into transacting with them.

US

Spoofing can result in civil/regulatory as well as criminal liability.

In 2010, the Dodd-Frank Act amended the Commodity Exchange Act (CEA) to include spoofing as a disruptive practice in commodities trading. The anti-spoofing provision makes it unlawful for any person to engage in spoofing which is defined as "bidding or offering with the intent to cancel the bid or offer before execution."

In a civil enforcement action, it is necessary to prove that the trader acted with a degree of intent that goes "beyond recklessness." However, US (and UK) exchanges and trading venues recognise several permissible order-obscuring or cancellation practices, such as iceberg orders, "fill or kill" orders, or "all or none" orders. Drawing a bright line between these permissible practices and an alleged incident of spoofing is a challenge.

First published on the *Global Investigations Review* website, 21 May 2020.

CFTC guidance identifies four non-exclusive examples of spoofing-like practices. These are the submission or cancellation of bids or offers to: overload the quotation system of a CFTC registered entity; delay another person's execution of trades; create an appearance of false market depth; or create artificial price movements upwards or downwards.

The CFTC may bring spoofing cases against individuals or firms. Notably, CFTC Regulation 166.3 requires each CFTC registrant to diligently supervise the handling by its partners, officers, employees and agents of all commodity interest accounts and activities relating to its business as a registrant. Spoofing-like conduct by individual traders may result in the firm incurring "failure to supervise" liability.

In the securities context, the SEC can bring civil enforcement actions for spoofing under the general anti-manipulation and anti-fraud provisions of the Exchange Act and the Securities Act.

The DOJ can prosecute the same CEA, Exchange Act and Securities Act provisions criminally. In a criminal prosecution under the CEA, it is necessary to prove that the trader knowingly acted with specific intent to cancel at the time the order was placed. Given the variety of legitimate reasons a trader might have to cancel an order prior to execution, and the difficulty of evidencing knowing intent, this is a high hurdle. Prosecutions may also be mounted using the commodities fraud statute and traders have also been charged with violating the wire fraud statute.

US prosecutors have recently augmented spoofing prosecutions with the Racketeer Influenced and Corrupt Organizations Act (RICO). Indictments have described an alleged conspiracy by traders engaged (as a criminal enterprise) in a pattern of racketeering activity. This is a significant escalation of US prosecution tactics. The RICO statute was initially created to disrupt and prosecute organised crime families engaged in disparate conduct like extortion, bribery, gun-running, violent assaults and murder. While RICO has been used in a white-collar context on previous occasions, the DOJ's decision to deploy it against spoofing indicates not only how seriously it takes the prosecution of spoofing, but also the difficulties it has encountered convincing juries to convict traders using the anti-spoofing statute, as well as complications imposed by relevant statutes of limitations.

US enforcement of spoofing: last five years
1 criminal conviction
8+ guilty pleas
1 acquittal

First published on the *Global Investigations Review* website, 21 May 2020.

1 mistrial
7+ individual civil settlements
4 civil settlements with firms at the same time as their key trader
15+ civil settlements with firms

UK

In the UK there is no dedicated anti-spoofing statute or offence. However, spoofing in a securities or commodities context falls squarely within the ambit of the EU Market Abuse Regulation (MAR) – which has direct effect in the UK (at least until the end of the Brexit transition period). Moreover, sections 89 and 90 of the Financial Services Act 2012 (FSA 2012), as well as section 2 of the Fraud Act 2006, provide avenues for criminal prosecution of market manipulation.

Article 15 of MAR outlaws market manipulation and attempted market manipulation, with articles 12 (1) and (2) describing impermissible transactions, orders or behaviours that encompass spoofing-like conduct. This includes conduct (such as the placement or cancellation of orders) which gives, or is likely to give, false or misleading signals as to the supply of, demand for, or price of a security or commodity; secures, or is likely to secure, the price of a security or commodity at an abnormal or artificial level; employs a fictitious device or any other form of deception or contrivance; disrupts or delays (or is likely to disrupt or delay) the functioning of the trading system of a trading venue; or overloads or destabilises the order book, or otherwise makes it difficult for other persons to identify genuine orders.

There is no requirement in MAR to prove that a trader intended, at the moment of order placement, to cancel the order prior to execution. Rather, MAR focuses on the market impression or effects of a particular transaction, order or course of conduct, notwithstanding what the trader's intent may have been. This creates a clear distinction between the UK and US enforcement regime, and arguably a more forgiving evidential burden in the UK (at least in the regulatory context).

Section 89 (false or misleading statements) and section 90 (false or misleading impressions) of FSA 2012 create criminal liability for spoofing. While these provisions require elements of intent or dishonesty to be proved, as with MAR there is no explicit requirement to prove that a trader intended (when placing an order) to cancel it before execution.

Why the disparity?

US authorities have exhibited sustained (and in some cases surprising) prosecutorial zeal when it comes to spoofing, despite encountering various setbacks along the way.

First published on the *Global Investigations Review* website, 21 May 2020.

Regulatory and civil enforcement is, of course, entirely appropriate when traders are caught actively engaging in misleading or disruptive practices on electronic markets. However, the decision to prosecute criminally is a grave one, especially in situations where the markets can be safeguarded, and the public interest adequately served, by civil or regulatory proceedings.

In situations where there is industrial-level, technology-enabled spoofing – affecting multiple trading counterparties – (as in *US v Coscia*), criminal prosecution is clearly warranted. However, other cases are not so clear, including those involving manual traders, limited or ambiguous incidents, or where "pinging" orders are entered for the purposes of price discovery in opaque markets dominated by algorithms. It is not surprising that juries (to date) have refused to convict manual traders for what may strike many jurors – at worst – as a "victimless" form of bluffing in computer-dominated markets. It remains to be seen whether upping the stakes with wire fraud and RICO will alter that dynamic.

For similar reasons, it is not necessarily surprising that there have been no UK criminal cases to date. The FCA does not often use its criminal powers in any context, and it may well be prioritising its criminal focus on other, arguably more pernicious, conduct such as money laundering. As for the Serious Fraud Office (SFO), its caseload tilts heavily in the direction of international bribery & corruption and other forms of complex international fraud where there is an obvious (and often vulnerable) economic victim, or where a corporate deferred prosecution agreement can be negotiated. When it comes to prosecuting traders, the SFO has for many years focused on the Libor manipulation scandal, as well as other financial-crisis era conduct – but with only limited success. Given this track record, the difficulty in proving criminal-level spoofing, and the likely jury reaction of "who cares if one trader is bluffing another trader" (not to mention a computer), we do not expect the SFO to open up a "spoofing" division anytime soon.

What is perhaps more surprising is the relatively sparse record of regulatory enforcement by the FCA, particularly when it does not have to prove the element of intent that exists in US law. After an initial flurry of activity between 2013 and 2015 that largely focused on high-frequency traders, the FCA's inaction in this area is notable in comparison to US regulatory enforcement. Caution in pursuing criminal prosecutions is understandable given how difficult it is to prove that a cancelled order is an abusive or disruptive one – especially in the manual trading context. But with the continued proliferation of high-frequency and algorithmic trading technologies, and the general volatility and disruption in the markets, it is hard to believe that there aren't more Michael Coscias out there making a killing.

Editor's note: Partner Zach Fardon led the US Attorney's Office for the Northern District of Illinois in Chicago when it successfully prosecuted Michael Coscia in 2015.

First published on the *Global Investigations Review* website, 21 May 2020.