CLIFFORD
CHANCE

Client briefing November 2015

# Spoofing: the first criminal conviction comes in the US – perspectives from the US and UK

US authorities have secured their first criminal conviction for the spoofing offense added to the US Commodity Exchange Act by the Dodd Frank Act. Following the conviction commentators have expressed concern that, as authorities on both sides of the Atlantic seek to increase the number of spoofing cases they pursue, they may find it difficult to distinguish between traders who are spoofing and those pursuing legitimate trading strategies. Against that background we recap the scope of the US anti-spoofing offense and compare the position in the US to the position in the UK where, unlike in the US, civil liability for spoofing can be incurred without a showing of intent.

## Recent Conviction in the US

On November 3, 2015 Michael Coscia, the founder of Panther Energy Trading, was convicted in Chicago federal court of six counts of spoofing and six counts of commodities fraud.

At the seven-day trial the jury heard that Coscia had engaged in spoofing in the markets of various commodities, including gold, soybean meal, soybean oil, high-grade copper, Euro FX and Pounds FX currency futures using an algorithm. The US Department of Justice ("DOJ") has indicated that in less than three months in 2011, Coscia illegally profited nearly $1,400,000.

This is the first criminal conviction under the anti-spoofing provision added to the US Commodity Exchange Act ("**CEA**") by the Dodd Frank Act of 2010, and follows civil and disciplinary actions taken against Coscia in 2013 by the Commodity Futures Trading Commission ("**CFTC**") and Chicago Mercantile Exchange ("**CME**") respectively in the US as well as the Financial Conduct Authority ("**FCA**") in the UK, in which Coscia and Panther Energy Trading paid total penalties of $3,700,000. The criminal case was prosecuted by a new unit of the Northern District of Illinois US Attorney's Office in Chicago called the Securities and Commodities Fraud Section, which was formed in April 2014.

Following Coscia's criminal conviction, Timothy Massad, chair of the CFTC, has emphasized that the CFTC will continue to treat spoofing as a priority and that traders "*should talk to their lawyers*" if "*they're entering a lot of orders without the intention to consummate*." We expect that, for the foreseeable future, we will continue to see the CFTC bringing civil actions for spoofing and referring appropriate cases to the DOJ for prosecution.

What distinguishes spoofing from otherwise legitimate trading is the trader's intent at the time of placing the order. Therefore, in some cases, the line between permissible conduct and a violation may be less than perfectly clear. As criminal prosecutions and civil enforcement actions for spoofing become more commonplace, it may be difficult for traders and counsel to discern the difference between legitimate trading practices and prohibited spoofing.

With these concerns in mind, we examine the scope of the spoofing offense as the law currently stands in the US and the UK.

## US Statutory Regime and Official Guidance

The CEA's anti-spoofing provision prohibits conduct that is "commonly known" as "spoofing," which is defined as "bidding or offering with the intent to cancel the bid or offer before execution."[1] The offense can be prosecuted as a civil violation by the CFTC or, in appropriate matters, as a criminal offense by the DOJ (to whom the CFTC will often refer matters having conducted preliminary investigations). Any purposeful violation of the CEA is punishable as a criminal offense. Each count of criminal spoofing carries a maximum penalty of 10 years in prison and a $1,000,000 fine.[2]

The defining aspect of spoofing is the trader's intent at the time of placing the order. If a trader intended to cancel an order at the time they placed the order, they engaged in spoofing. If, on the other hand, they intended to fill the order, but were unable to do so, the placement of the order was not spoofing. Although the allegations in the US cases pursued to date suggest that the CFTC has clear evidence that the traders were placing orders with intent to cancel the trade in a deliberate attempt to mislead the market, intent to mislead the market is not a necessary element of the offense.

Under the CEA, the CFTC is empowered to issue rules and guidance necessary to enforce the primary provisions of the CEA. In 2013, the CFTC issued rules and interpretive guidance in relation to the anti-spoofing provision. In that guidance, the CFTC made the following points:

1. The CFTC considers that a market participant must act with some degree of intent beyond recklessness to engage in the spoofing trading practices prohibited by the CEA;
2. The CFTC considers that a spoofing violation will not occur where the person's intent when cancelling a bid or offer before execution was to cancel such bid or offer as part of a legitimate, good faith attempt to consummate a trade;
3. The CFTC does not consider that a pattern of trading is necessary for a violation to occur: spoofing may be committed with a single order. However, in determining whether spoofing has occurred, the CFTC will look at all the facts and circumstances of a case including an individual's trading practices and patterns where applicable.

In the same guidance, the CFTC provided four non-exclusive examples of spoofing behavior: (i) submitting or cancelling bids or offers to overload the quotation system of a registered entity; (ii) submitting or cancelling bids or offers to delay another person's execution of trades; (iii) submitting or cancelling bids or offers with intent to create artificial price movements; and (iv) submitting or cancelling multiple bids or offers to create an appearance of false market depth.

The CFTC guidance has left significant uncertainty about the requirements of proof. In particular, it provides that the trader's state of mind must be "beyond reckless," but leaves open whether actual intent is required for a CEA civil spoofing violation. Thus, CFTC may take the view that a trader could be "beyond reckless" in placing an order, even if there was no intent to cancel the order when it was placed. In contrast the standard in criminal prosecutions is more clear. The CEA expressly states that a willful violation of that statute or CFTC rules are felonies prosecutable by the DOJ. There, the DOJ, which is required to prove its cases beyond a reasonable doubt unlike the CFTC's mere preponderance of evidence standard, will need to establish that the trader had the specific intent to cancel or modify an order to avoid trade consummation at the time the order was placed.

---

1 CEA § 4c(a)(5)(C).

2 Note that each count of commodities fraud for which Coscia was also convicted carries a maximum sentence of 25 years in prison and a $250,000 fine.

Nevertheless, the CFTC guidance suggests that the CFTC will prioritize cases where specific intent is present, as reflected by trading that appears to be motivated by a desire to mislead, as the examples in the guidance appear to involve such activity (e.g. "submitting or cancelling bids or offers *with intent to create artificial price movements*"). However, these are non-exhaustive examples and the CFTC could conceivably bring an enforcement action alleging spoofing conduct outside the context of market deception.

Indeed, viewed from another perspective the examples in the guidance give less comfort because they involve scenarios that would go beyond the scope of the statute absent some evidence that the trader intended not to execute the orders at the time they were placed. For example, submitting bids with intent to overload the quotation system of a registered entity arguably goes beyond the statute, as a trader could, in theory, place these offers with the intent to execute them. Furthermore the guidance provides that "*a section 4c(a)(5)(C) violation occurs when the trader intends to cancel a bid or offer before execution*" which, as written, could include a circumstance where a trader simply changes his mind about whether to execute a bid or offer previously placed. Therefore, a prudent reading of these examples suggests they should be confined to bids and offers made with a concurrent intent to cancel before execution.

The US exchanges have also published their own rules and guidance on spoofing. For example the CME and ICE have published guidance on what conduct may constitute spoofing under CME Rule 575 and Intercontinental Exchange ("**ICE**") Rule 4.02 respectively. Like the statutory language, this guidance focuses on intent, and suggests that exchanges will focus on whether deception or market abuse occurred. Specifically, the exchanges will consider, among other things: (i) whether the market participant's intent was to induce others to trade when they otherwise would not; (ii) whether the market participant's intent was to affect a price rather than to change his position; (iii) whether the market participant's intent was to create misleading market conditions; and (iv) the ability of the market participant to manage the risk associated with the order(s) if fully executed, in determining whether conduct constitutes spoofing.

Liability for spoofing can also extend to employers. The CEA provides that companies are liable for the acts of their agents that are "within the scope of [their] employment or office."[3] In the Coscia matter, the CFTC's final order stated that both Coscia and Panther Energy Trading violated the CEA's anti-spoofing provision by designing an algorithmic trading program to place orders giving the impression of market interest on one side of the market. However, it is not clear from the order whether the CFTC relied on a *respondeat superior* theory in holding Panther Energy Trading liable.

As a rule, the CFTC will seek to hold a company liable for actions of employees where employees are acting within the scope of their employment. Similarly, companies may face criminal prosecution for the conduct of their employees. The decision whether to prosecute a company will be guided by the DOJ's corporate prosecution policies as set forth in the Filip factors and the recently released Yates memorandum. To date, there have been no corporate criminal prosecutions under the new anti-spoofing provision, but it is conceivable that such criminal prosecutions may be easier in respect of spoofing committed by algorithmic trading, given that the design and use of an abusive algorithm is more likely to involve enterprise level decision-making.

## Pending US Prosecutions and Enforcement Actions for Spoofing

It is understood that the CFTC currently has three further spoofing cases in the pipeline, two of which are directed against traders located outside the US. The CFTC has sought the extraordinary remedy of a preliminary injunction in all three cases.

A spoofing-related civil enforcement action and criminal complaint against UK national Navinder Singh Sarao were unsealed on April 21, 2015 in Chicago federal court. Sarao is accused of engaging in spoofing of E-mini S&P 500 futures traded on the CME (using an algorithm) and causing the so-called Flash Crash in 2010. Sarao allegedly utilized an automated system to layer large

---

[3] CEA § 2(a)(1)(B).

and numerous sell orders, causing price swings that Sarao would then profit from. According to the criminal complaint against him, Sarao would also "flash" and quickly cancel large lot orders to amplify the price impact of his layering algorithm. In its complaint, the CFTC asked for a permanent injunction to prevent Sarao and his company from trading in any markets or on any entity regulated by the CFTC. Mr. Sarao is currently the subject of extradition proceedings in the UK.

On May 5, 2015, the CFTC filed a civil enforcement action in New York federal court against Heet Khara and Nasim Salim, both residents of the United Arab Emirates. Khara and Salim were accused of spoofing in the gold and silver futures markets (specifically COMEX) from at least February 2015 through at least April 28, 2015. Khara and Salim's alleged misconduct included working in tandem to enter a large quantity of orders on one side of the market while having at least one smaller order on the opposite side of the market. Once the small order(s) traded, they would allegedly cancel the numerous orders on the opposite side. The CME suspended Khara and Salim from trading on April 30, 2015. On May 14, 2015, the New York judge presiding over the case took the extraordinary step of issuing a preliminary injunction against Khara and Salim, precluding the individuals from trading in commodities, freezing the defendants' assets, and ordering that the CFTC have access to and inspect the defendants' books and records.

On October 19, 2015, the CFTC filed an anti-spoofing complaint against Igor Oystacher and his firm 3Red Trading LLC in Chicago federal court alleging spoofing of various CME futures. The CFTC alleges that Oystacher placed large orders on one side of the market at or near the best price, which were intended to be canceled before execution. According to the CFTC, Oystacher would use a feature in his trading software, to cancel the orders and "flip" his position by placing at least one aggressive order on the other side of the market to trade with participants that had been induced to enter the market by the spoof orders. On November 9, 2015, the CFTC filed a motion for preliminary injunction seeking to prevent Oystacher from trading futures contracts while the case against him is pending. This is an extraordinary remedy, which is rarely used to prevent a US trader from trading on a US exchange due to alleged violations of the CEA's anti-spoofing provisions.

In each of these cases the allegations appear to involve "classic" spoofing tactics that evidenced a clear present intent not to execute the orders made, in an attempt to mislead other market participants. It remains to be seen, therefore, whether US authorities will pursue less obvious cases using the broadest readings of the statutory wording and CFTC guidance.

# The position in the UK

As noted above, Coscia was also punished in the UK for spoofing. On July 3, 2013 the FCA imposed a fine of £597,993 on Mr. Coscia for using an algorithm to engage in spoofing in the markets for Brent Crude Futures, Gas Oil Futures, and Western Texas Intermediate Crude Futures on ICE Futures Europe over a six week period in 2011.

Since Coscia's punishment, there have been two further spoofing cases in the UK: (i) on January 24, 2014 the FCA imposed a fine of £8,000,000 on Canadian company Swift Trade Inc for systematically spoofing a wide range of shares on the London Stock Exchange (the "LSE") during 2007 and 2008; and (ii) on August 12, 2015 the High Court, following a claim by the FCA, imposed penalties totaling £7,600,000 on the English branch of a Swiss hedge fund, Da Vinci Invest Limited, three traders based in Hungary, and a Seychelles company controlled by those traders for spoofing a wide range of shares on the LSE in late 2010.

## Civil regime

In each of Coscia, Swift Trade, and Da Vinci, the FCA took action using its powers under the civil market abuse regime set out in Part VIII of the UK Financial Services and Markets Act 2000 ("**FSMA**"), which implements the provisions of the European Market Abuse Directive. The basis of the action in each case was section 118(5) of FSMA, which provides that one of the behaviors which may amount to market abuse:

"*consists of effecting transactions or orders to trade (otherwise than for legitimate reasons and in conformity with accepted market practices on the relevant market) which –*

*a) give, or are likely to give, a false or misleading impression as to the supply of, or demand for, or as to the price of, one or more qualifying investments, or*

*b) secure the price of one or more such investments at an abnormal or artificial level.*"

Much like the CFTC, the FCA has published a code giving guidance as to conduct which it considers is or is not market abuse (the Code of Market Conduct ("COMC")). COMC does not refer to spoofing, but it does describe spoofing-like behavior. Paragraph 1.6.2 provides that "*entering orders into an electronic trading system, at prices which are higher than the previous bid or lower than the previous offer, and withdrawing them before they are executed, in order to give a misleading impression that there is demand for or supply of the qualifying investment at that price*" is considered by the FCA to be market abuse within the meaning of section 118(5) of FSMA. The High Court relied on this paragraph in Da Vinci to support its decision.

Unlike the US anti-spoofing statute, under the UK civil market abuse regime there is no intent requirement of any kind. The English courts have held that "*the test is wholly objective; it does not require any particular state of mind on the part of the person whose behaviour is under consideration*."[4]

On the facts, both Coscia and Swift Trade were found by the FCA to have engaged in spoofing deliberately, intending to mislead the market. However, in Da Vinci, the High Court found that Da Vinci Invest Limited had engaged in spoofing falling within the scope of section 118(5) without intent to mislead the market or to commit market abuse. Da Vinci management were found to have been unaware of the abusive trading strategy employed by its traders, but, since the orders and trades were in Da Vinci's name, Da Vinci was found to have committed market abuse, regardless of its lack of intent because the civil regime in the UK is effects-based. Da Vinci was found to have been reckless in allowing traders to trade in its name without properly performing due diligence on them or their trading strategy. But that recklessness went to penalty rather than liability.

Note that Da Vinci would also have been likely to face civil liability under US law, but for different reasons. There, as discussed above, the intent of its traders would have been imputed to the entity under a vicarious liability theory, thus satisfying the intent requirement for the entity. Conversely in the UK under the civil and criminal market abuse regimes, if intent must be proved against a corporate entity, that intent must be found in an employee sufficiently senior to constitute the company's "directing mind and will."

Beginning July 2016, the civil anti-spoofing provisions applicable in the UK will derive directly from the new European Market Abuse Regulation—which comes into force then—rather than from FSMA. However, the substance of the provisions relevant to spoofing will remain the same and liability will continue to be effects-based, without any intent requirement.

## Criminal regime

Unlike in the US, there has been no criminal prosecution for spoofing in the UK to-date, but there are separate provisions of criminal law which would allow prosecution to take place.

Under section 90 of the Financial Services Act 2012 ("**FSA 2012**") a person commits an offense if (in summary) he does any act which creates a false or misleading impression as to the price of any relevant investments, if he intends to create the impression, and either: (i) he intends to induce another person to acquire or dispose of those investments or to refrain from doing so; or (ii) he knows that the impression is false or misleading or is reckless as to whether it is, and intends to make a gain or to cause a loss to another. The offense applies where the act is done in the UK, or the false or misleading impression is created there. It is punishable by up to 7 years in prison and an unlimited fine.

The full wording of section 90 is complicated and its meaning has not been considered by the Courts, but it is clear that its scope is more similar to the offense under the US CEA than the provisions of the UK civil regime discussed above.

---

[4] Winterflood Securities Limited v FSA [2010] EWCA Civ 423, per Moore-Bick LJ at [25].

In particular it appears that whilst section 90 does require intent to create an impression, it does not require an intention to create a misleading impression.

If that construction is right the UK may in due course see criminal prosecutions for spoofing in which the defendant is accused only of having been reckless as to whether his trading would give a false or misleading impression to the market. It is conceivable that such allegations might be made in circumstances where a trader has used an algorithm to trade without properly understanding how the algorithm works, being reckless as to whether it would mislead the market, or in circumstances where a company allows a trader to trade on its behalf being reckless as to whether that trader would employ a misleading trading strategy.

Note that section 90 FSA 2012 replaced section 397(3) FSMA which established a similar offense but which required a prosecutor to prove that a person had acted for the purpose of creating a false or misleading impression, and for the purpose of inducing a person to deal in relevant investments or to refrain from doing so. The language of the old section arguably poses a significantly higher hurdle for a prosecutor to overcome.

Following the conviction of Michael Coscia in the US, and given the growing appetite in the UK for harsher punishment for those who engage in market abuse (see for example the Fair and Effective Markets Review published by the FCA, Prudential Regulation Authority and Bank of England in June 2015 which calls for the increase of the maximum sentence for criminal market abuse from 7 to 10 years), it is to be expected that we will soon see prosecutions under section 90 FSA 2012 for spoofing. Those are likely to be easier to achieve under section 90 than they would have been had section 397 remained in force. The FCA may have a greater appetite for pursuing a prosecution in those circumstances.

Whether Navinder Singh Sarao could be prosecuted in the UK for his alleged spoofing of the market for E-mini S&P 500 futures traded on the CME, given that he is said to have traded from his home in London, may well become an issue in his extradition proceedings. The question will need to be determined by reference to section 397(3) given that the conduct in question occurred in 2010, but any analysis by the court as to the scope of section 397(3) would also be relevant to future applications of section 90 FSA given the similarity between the two provisions.

# Conclusion

Spoofing remains at the top of the regulatory agenda on both sides of the Atlantic. We are likely to see an increasing number of civil and criminal enforcement actions against those who engage in spoofing and most if not all of these are likely to involve traders using algorithms and high frequency trading strategies. To-date, enforcement cases in both jurisdictions have involved scenarios that demonstrate misconduct that neatly falls within the statutory language. However, if authorities are to take on a greater number of spoofing cases, we may soon see the breadth of the anti-spoofing provisions in both jurisdictions tested. In the meantime, market participants would gratefully receive any further guidance that the authorities can offer regarding the scope of the offense.

## Authors

**Carlos Conceicao**
Partner, London

T: +44 20 7006 8281
E: carlos.conceicao
@cliffordchance.com

**Robert Houck**
Partner, New York

T: +1 212 878 3224
E: robert.houck
@cliffordchance.com

**Christopher Morvillo**
Partner, New York

T: +1 212 878 3437
E: christopher.morvillo
@cliffordchance.com

**Kelwin Nicholls**
Partner, London

T: +44 20 7006 4879
E: kelwin.nicholls
@cliffordchance.com

**David Yeres**
Senior Counsel, New York

T: +1 212 878 8075
E: david.yeres
@cliffordchance.com

**Benjamin Berringer**
Associate, New York

T: +1 212 878 3372
E: benjamin.berringer
@cliffordchance.com

**Oliver Pegden**
Senior Associate, London

T: +44 20 7006 8160
E: oliver.pegden
@cliffordchance.com



Clifford Chance, 31 West 52nd Street, New York, NY 10019-6131, USA



www.cliffordchance.com