THOMSON REUTERS
PRACTICAL LAW™

"Spoofing" the market: a comparison of US and UK law and enforcement

by *Aaron Stephens* (Partner, London), *Zach Fardon* (Partner, Chicago), *Katherine Kirkpatrick* (Partner, Chicago), *Rob Dedman* (Partner, London), *Michael Watling* (Partner, New York), *Matthew Wissa* (Associate, Chicago), and *Margaret Nettesheim* (Associate, London), King & Spalding LLP

This document is published by Practical Law and can be found at: **uk.practicallaw.com/w-020-1043**
To learn more about legal solutions from Thomson Reuters, go to **legal-solutions.co.uk**

This practice note provides an overview of the application and enforcement of the US and UK legal and regulatory regimes in relation to the manipulative trading behaviour known as "spoofing".

RESOURCE INFORMATION

RESOURCE ID
w-020-1043

RESOURCE TYPE
Practice notes

STATUS
Maintained

JURISDICTION
United Kingdom
United States

Scope of this note

Recently, the US Commodities Futures Trading Commission (CFTC), the US Department of Justice (DOJ), and the UK Financial Conduct Authority (FCA) have stepped up their efforts to pursue market participants for manipulative trading behaviour in the securities and commodities markets. For example, the CFTC's Director of Enforcement, James McDonald, released a *statement* in January 2018 announcing the CFTC's efforts to combat market manipulation in relation to spoofing. Similarly, in February 2019, Julia Hoggett, the FCA's Director of Market Oversight, delivered a *speech* about the FCA's commitment to tackling market abuse.

This practice note summarises and compares US and UK law and enforcement on the topic of spoofing. Specifically, the note describes how each jurisdiction's enforcement bodies prosecute spoofing under applicable law and provides examples of the types of trading practices that may constitute spoofing.

What is "spoofing"?

Spoofing is a form of market manipulation whereby a trader submits and then cancels offers or bids in a security or commodity on an exchange or other trading platform with no intent or willingness to execute those orders when placed. To put it another way, spoofing occurs where a trader places an order with the co-existent intent to cancel the bid or offer before it can be executed.

Spoofing may take various forms, but it often involves the placing of non-bona fide, large or small volume orders on one side of the order book, and then cancelling those orders either immediately or within a very short period of time after placement. A spoofing trader's intent may be to alter the appearance of supply or demand to artificially move the price and thus mislead - or spoof - other traders in the relevant security or commodity, and thus benefit his or her own trading position(s). Spoofing is also referred to as "layering" the order book, which involves the trader placing multiple, non-bona fide orders on one side of the order book to manipulate the price and thus benefit their position(s) on the other side of the order book.

Spoofing often utilises algorithmic and high frequency trading technology, which allows trading decisions to be generated quickly and transactions to be completed in fractions of a second. In general, algorithmic and high frequency trading are legitimate trading strategies. However, regulators have scrutinised algorithmic trading methods and consider some to be market manipulation.

In the US, spoofing is a specified criminal and civil offence, and other provisions of the securities laws may also be used to enforce against spoofing-like behaviour.

In the UK, spoofing is not a specified offence. However, spoofing behaviour may contravene civil and/or regulatory provisions in the EU *Market Abuse Regulation (596/2014)*(MAR) (which has direct effect in the UK) and/or amount to a criminal offence under the *Financial Services Act 2012* (FS Act 2012) or the *Fraud Act 2006*.

In the US, the trader's intent is pivotal. To prosecute spoofing, US authorities must prove that there was intent to cancel the order at the time it was placed. In the UK, authorities generally focus on the impact of the spoof order on the market. While there is limited UK case law to date, in general terms the trader's intent may be irrelevant (in a UK civil case) or less central (in a UK criminal case) than in a case under US law.

Differences between US and UK spoofing law and enforcement: at a glance

US and UK law on spoofing

	US	UK
Enforcement authorities	• CFTC (civil). • Securities and Exchange Commission (SEC) (civil). • Financial Industry Regulatory Authority (FINRA) (civil). • DOJ (criminal).	FCA (civil and criminal)
Current law	• Dodd-Frank Act 2010, Section 747. • Commodity Exchange Act (CEA), Section 4c(a)(5)(C). • Securities Exchange Act of 1934 (Exchange Act), Sections 10(b) and 9(a)(2). • Securities Act of 1933 (Securities Act), Section 17(a). • SEC Rule 10b-5. • FINRA Rule 2020.	• *MAR*, Article 15. • *FS Act 2012*, sections 89 and 90. • *Fraud Act 2006*.
Key differences	• US law includes specific civil and criminal anti-spoofing provisions. • **Intent:** In all cases, requires proof of the individual's intent to cancel the bid or offer before execution. • In **civil** cases brought by the CFTC, individuals must be found to have acted "with some degree of intent, or scienter, beyond recklessness." (78 Fed. Reg. at 31896.) The standard of proof for civil cases is proof by a preponderance of the evidence. • In **criminal** cases brought by the DOJ, in addition to the intent standard above, the prosecutor must prove the individual "knowingly" engaged in spoofing. The DOJ may bring criminal charges relating to spoofing under the CEA, or instead, under the mail, wire, and commodities fraud statutes. (7 U.S.C. § 13(a)(2). CEA § 9(a)(2).) The standard of proof for criminal cases is proof beyond a reasonable doubt.	• UK law does not include any specific anti-spoofing provisions; rather, spoofing behaviour is generally construed to be a form of **market manipulation** that may result in civil or criminal liability. • **Intent:** differs between the civil and criminal regimes (see *Offences and enforcement framework: UK* below). • In a **civil** case, the FCA must only prove that the behaviour created a false or misleading impression in the market, regardless of the trader's intent when placing the order or more generally (see *Offences* below). • In a **criminal** case under the FS Act 2012, a prosecutor must prove that the behaviour had an actual effect on the market and must also prove some element of intent (that is, that the defendant intended by his or her behaviour to create an impression on the market, but did not necessarily intend to create a misleading impression). In contrast to the US, the law does not on its face require a prosecutor to prove that the trader had the specific intent to cancel the order before it could be executed (see *FS Act 2012* below), although this proposition remains untested. • A prosecution under the Fraud Act 2006 would require a slightly different element of proof with regard to intent (see *Fraud Act 2006* below).

Note that MAR is complemented by the *Directive on Criminal Sanctions for Market Abuse (2014/57/EU)* (CSMAD), which participating member states were required to transpose into national law by 3 July 2016. However, the UK government decided not to opt in to CSMAD and therefore the UK did not transpose its provisions into national law. Accordingly, this note does not consider the provisions of CSMAD.

For an overview of MAR, see *Practice note, Market Abuse Regulation (MAR): overview*. For an overview of CSMAD, see *Practice note, Directive on Criminal Sanctions for Market Abuse (CSMAD)*.

Legal trading strategies and spoofing

As noted, to constitute a spoofing offence under US law, the trader must have simultaneously intended (at the time of order placement) to cancel his or her bid or order before execution. However, there are a number of legitimate, legal trading strategies in which bids or orders are cancelled before execution, and most orders in the securities and commodities markets go unfilled. The CFTC has set out under the CEA which trading strategies are legal and which trading cancellation strategies are illegal. As such, prosecutors must distinguish between legitimate and illegitimate trading activities in which traders cancel their bids or offers to determine whether the cancelled trade may constitute spoofing.

The following sections set out non-exclusive lists of different types of trading practices, legal and illegal, that utilise cancellation methods. The legal practices are common on both US and UK exchanges.

Legal order cancellations

- **Fill or kill (FoK) order.** This is an order that demands immediate execution or cancellation, typically involving a designation added to an order instructing the broker to offer or bid (as the case may be) one time only; if the order is not filled immediately it is then automatically cancelled.
- **Stop-loss (or stop-limit) order.** This is an order that goes into force as soon as there is a trade at the specified price. The order can only be filled at the stop price or better.
- **All or none (AON) order.** This is an order to buy or sell a stock that must be executed in its entirety or not executed at all. However, unlike the FoK orders, AON orders that cannot be executed immediately remain active until they are executed or cancelled.
- **Iceberg order (hidden quantity order).** This is an order placed on an electronic trading system whereby only a portion of the order is visible to other market participants. As the displayed part of the order is filled, additional portions of the order become visible.
- **Passive order.** This is an offer to sell at a price that is higher than the price at which other traders are currently willing to buy. Passive orders rest for at least some amount of time after being placed and are not guaranteed to execute.

Illegal order cancellations

- **Spoofing.** As noted in *What is "spoofing"?* above, spoofing means placing a non-bona fide order or orders with the simultaneous intention of cancelling the order(s) before they can be executed, in order to disrupt or manipulate a relevant market.
- **Layering.** This term refers to placing multiple non-bona fide orders (that are designed not to trade) on one side of the order book.
- **Wash trading.** This involves entering into, or purporting to enter into, transactions that give the appearance that purchases and sales have been made, without actually incurring market risk or changing the trader's market position.

Offences and enforcement framework: US

Commodity Exchange Act (CEA)

The CFTC enforces the civil provisions of the CEA, including the anti-spoofing provision, while the DOJ has the authority to criminally prosecute spoofing violations of the CEA, as well as the federal mail and wire fraud statutes.

For more information, see the CFTC's *interpretative guidance and policy statement on disruptive practices* (CFTC Guidance).

In addition to the CFTC Guidance, certain US exchanges have also published rules and guidance on what constitutes spoofing. For example, the Chicago Mercantile Exchange (CME) has published a *market regulation advisory notice* (CME Group RA1807-5), and Intercontinental Exchange (ICE) Futures US has published a set of *FAQs on disruptive trading practice*.

Offences

In 2010, the Dodd-Frank Act amended the CEA to include spoofing as a disruptive practice. The anti-spoofing provision, CEA Section 4c(a)(5)(C), makes it unlawful for any person to engage in spoofing, which is formally defined as "bidding or offering with the intent to cancel the bid or offer before execution." *7 U.S.C. § 6c(a)(5)(2012).*

The CFTC Guidance suggests four non-exclusive examples of situations that may constitute spoofing:

- Submitting or cancelling bids or offers to overload the quotation system of a registered entity.

- Submitting or cancelling bids or offers to delay another person's execution of trades.
- Submitting or cancelling multiple bids or offers to create an appearance of false market depth.
- Submitting or cancelling bids or offers with intent to create artificial price movements upwards or downwards.

To constitute spoofing, the trader must act with the specific (or at least "beyond reckless") intent to cancel the bid or offer prior to execution.

In civil cases, it is somewhat ambiguous as to whether this means "specific intent" (as understood in US law to be the subjective desire or knowledge that the prohibited result will occur (see *People v. Owens, 131 Mich. App. 76, 345 N.W.2d 904 [1983]*)) or some other standard of intent.

The CFTC Guidance states that:

> "The Commission interprets that a CEA section 4c(a)(5)(C) violation requires a market participant to act with **some degree of intent, or scienter, beyond recklessness** to engage in the "spoofing" trading practices prohibited by CEA section 4c(a)(5)(C). Because CEA section 4c(a)(5)(C) requires that a person intend to cancel a bid or offer before execution, the Commission believes that **reckless trading, practices, or conduct will not constitute a "spoofing" violation**." (Our emphasis added.)

In a criminal case, the DOJ must establish specific intent to cancel at the time the order was placed.

In any event, statistical data by itself is not enough for enforcers to demonstrate intent since it is common practice for traders to cancel orders and bids after they are placed, for a variety of legitimate purposes. On the other hand, a pattern of trading is not necessary for a violation to occur; in theory at least, a trader could spoof the market with a single order.

Under CFTC Regulation 166.3, an entity can be charged with a failure to supervise if its traders engage in spoofing. 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. Regulation 166.3 does not require proof of an underlying violation. Therefore, a firm can be found to have violated Regulation 166.3 even if there was ultimately no spoofing violation.

Penalties

- Spoofing under the CEA is a felony punishable by up to USD1 million in penalties and up to 10 years in prison for each spoofing count. *7 U.S.C. 13(a)(2).*
- Civil penalties or administrative sanctions may include orders imposing civil monetary penalties, suspending, denying, revoking or restricting registration and exchange trading privileges, orders of restitution, a receiver, a freeze of assets, restitution and disgorgement of unlawfully acquired benefits (see the *CFTC Enforcement Manual*).
- The CEA also provides that the CFTC may obtain certain temporary relief on an ex parte basis. When those enjoined violate court orders, the Division of Enforcement may seek to have the offenders held in contempt (see the *CFTC Enforcement Manual*).
- Violation of CFTC Regulation 166.3 can result in a USD25 million monetary civil penalty. *17 CFR § 166.3.*
- Certain individuals have entered into non-prosecution agreements (NPAs) (see, for example, this June 2017 CFTC *press release*).

Defences

Reckless trading practices do not violate CEA Section 4c(a)(5)(C). In addition, orders, modifications and cancellations are not considered spoofing if they are submitted as part of a legitimate, good faith attempt to consummate trading (for example, partially filled orders or properly placed stop-loss orders).

Exchange Act, Securities Act, FINRA Rules

The SEC can bring an enforcement action for spoofing under the general anti-manipulation and anti-fraud provisions of the Exchange Act and the Securities Act, with the DOJ pursuing parallel criminal prosecutions. In addition, FINRA member firms and associated individuals could face enforcement activity in relation to any breach of FINRA's rules.

Offences

Section 17(a) of the Securities Act prohibits the fraudulent sales of securities and makes it unlawful for any person in the offer or sale of any security or any security-based swap agreement, by the use of any means or instruments of transportation or communication in interstate commerce or by the use of the US mails, directly or indirectly, to do any of the following:

- Employ any device, scheme, or artifice to defraud.
- Obtain money or property by means of any untrue statement of a material fact or any omission to state a material fact necessary to make the statements made, in light of the circumstances under which they were made, not misleading.
- Engage in any transaction, practice, or course of business which operates or would operate as a fraud or deceit upon the purchaser. *15 U.S.C. § 77q(a).*

Section 9(a)(2) of the Exchange Act prohibits manipulation of securities prices and makes it unlawful

to effect, alone or with one or more other persons, a series of transactions in any security creating actual or apparent active trading in such security, or raising or depressing the price of such security, for the purpose of inducing the purchase or sale of such security by others. *15 U.S.C. § 78i.*

Section 10(b) of the Exchange Act prohibits fraud in connection with the purchase or sale of any security and makes it unlawful for any person, directly or indirectly, by the use of any means or instrumentality of interstate commerce or of the mails, or of any facility of any national securities exchange, to use or employ a manipulative or deceptive device or contrivance in contravention of such rules and regulations as the SEC may prescribe. *15 U.S.C. § 78j(b).*

Rule 10b-5 prohibits fraud, misrepresentation and deceit in connection with the purchase or sale of any security and makes it unlawful for any person, directly or indirectly, by the use of any means or instrumentality of interstate commerce, or of the mails or of any facility of any national securities exchange to use any device, scheme, or artifice to defraud. *17 C.F.R. 210.10b-5.*

FINRA Rule 2020 prohibits securities brokers and dealers from effecting any transaction in, or inducing the purchase or sale of, any security by means of any manipulative, deceptive or other fraudulent device or contrivance.

Penalties

- Wilful violations of the Securities Act or the Exchange Act are punishable by disgorgement and a civil fine of up to USD5,000,000 or imprisonment of not more than 20 years.
- For member firms, violations of FINRA Rule 2020 are punishable by censure, fine, suspension from securities activities in full or limited capacity for up to two years, or, in egregious cases, expulsion of the firm from FINRA membership. For associated individuals, such violations are punishable by censure, fine, suspension for up to two years, or permanent bar from FINRA membership.

US v Vorley and Chanu: challenge to spoofing charge under wire fraud statute

In July 2018, the DOJ indicted James Vorley and Cedric Chanu, two traders who worked at a global investment bank. The DOJ claimed that they had engaged in an illegal, years-long spoofing scheme that involved tricking other traders into buying or selling futures contracts at artificially inflated prices. However, instead of bringing charges under the CEA, which explicitly prohibits spoofing, the government brought charges solely under the federal wire fraud statute (Conspiracy to Commit Wire Fraud Affecting a Financial Institution in violation of 18 U.S.C. § 1349, and Wire Fraud Affecting a Financial Institution in violation of 18 U.S.C. § 1343).

The federal wire fraud statute includes a longer statute of limitations and greater penalties than the CEA. The government has argued that these charges were warranted because the defendants engaged *"in spoofing with fraudulent intent and in order to obtain money or property from someone else"*. The government has also sought to argue that a trader's order includes an "implicit representation" that they intend for the order to be filled, even though many orders are cancelled, and where the trader is not in a fiduciary relationship with any actual or potential counterparty. A false statement or material misrepresentation is a necessary element of wire fraud.

The Northern District of Illinois has yet to rule on the matter, but the defendants have filed a motion to dismiss the wire fraud charges. Several financial industry advocacy groups (including the Chamber of Commerce, the Bank Policy Institute, the Futures Industry Association, and the Securities Industry and Financial Markets Association) have filed amicus briefs supporting the defendants' position. Amongst other things, the amicus briefs argue that, with the CEA, Congress and the CFTC have established a comprehensive statutory and regulatory regime to govern the futures markets, and that the application of the wire fraud statute to open orders in those markets may adversely affect the proper and efficient functioning of the markets.

For more information, see this *DOJ press release* (dated 25 July 2018).

Offences and enforcement framework: UK

In the UK, spoofing is not a specified offence. Rather, the offence of market manipulation under Article 15 of *MAR* captures spoofing behaviour. In addition, there are criminal offences relating to market manipulation under sections 89 and 90 of the *FS Act 2012* and section 2 of the *Fraud Act 2006*.

Market Abuse Regulation (MAR)

The offence of market manipulation under Article 15 of *MAR* captures spoofing behaviour.

As noted above (see *Differences between US and UK spoofing law and enforcement: at a glance*), in the criminal context, MAR is complemented by *CSMAD*. However, as the UK government decided not to opt in to CSMAD, the criminal enforcement regime is purely a matter of UK domestic law.

The FCA is the competent authority in the UK for the purposes of MAR. As well as taking civil enforcement

action under MAR, the FCA can also bring criminal prosecutions for spoofing behaviour under the FS Act 2012 and/or the Fraud Act 2006 (see *FS Act 2012* and *Fraud Act 2006* below).

To date, the FCA (formerly the Financial Services Authority (FSA)) has only pursued civil enforcement action in relation to spoofing behaviour (see *Pre-MAR market manipulation offence* below). No criminal prosecutions for spoofing have been brought in the UK to date.

In February 2018, the FCA published a *report* on algorithmic trading compliance in wholesale markets. The report summarises the key areas of focus for algorithmic trading and highlights areas of good and bad practice observed in its reviews of firms' trading practices.

Pre-MAR market manipulation offence

Before MAR, market manipulation cases were pursued under section 118(5) of the *Financial Services and Market Act 2000* (FSMA), which contained the market abuse (manipulating transactions) offence. This covered behaviour that consisted of effecting transactions or orders to trade (otherwise than for legitimate reasons and in conformity with accepted market practices on the relevant market), which did either of the following:

- Gave, or were likely to give, a false or misleading impression as to the supply of, demand for, or price of one or more qualifying investments.
- Secured the price of one or more such investments at an abnormal or artificial level.

This offence and the other market abuse offences set out in section 118 of FSMA were repealed and replaced with effect from 3 July 2016, when MAR began to apply.

For more information on the former section 118(5) FSMA offence and examples of behaviour amounting to this, see *Practice notes, Market abuse: the types of behavior (pre-MAR regime): Manipulating transactions* and *Market abuse: examples of market manipulation (pre-MAR regime)*.

Offences

Article 15 of *MAR* makes it an offence to engage in market manipulation and attempted market manipulation.

Articles 12(1) and (2) MAR of specify that market manipulation includes spoofing-like activities and behaviour, namely:

- The entering into a transaction, placing an order to trade or any other behaviour which:
  - gives, or is likely to give, false or misleading signals as to the supply of, demand for, or price of, a financial instrument, a related spot commodity contract or an auctioned product based on emission allowances; or
  - secures, or is likely to secure, the price of one or several financial instruments, a related spot commodity contract or an auctioned product based on emission allowances at an abnormal or artificial level,

  unless the person entering into a transaction, placing an order to trade or engaging in any other behaviour establishes that such transaction, order or behaviour has been carried out for legitimate reasons, and conform with an accepted market practice (AMP) as established in accordance with Article 13 of MAR (*Article 12(1)(a)(i) and (ii), MAR*).
- The entering into a transaction, placing an order to trade or any other activity or behaviour which affects or is likely to affect the price of one or several financial instruments, a related spot commodity contract or an auctioned product based on emission allowances, which employs a fictitious device or any other form of deception or contrivance (*Article 12(1)(b), MAR*).
- The placing of orders to a trading venue, including any cancellation or modification thereof, by any available means of trading, including by electronic means, such as algorithmic and high frequency trading strategies, and which has one of the effects referred to in Article 12(2)(a) or (b) of MAR, by:
  - disrupting or delaying the functioning of the trading system of the trading venue or being likely to do so; or
  - making it more difficult for other persons to identify genuine orders on the trading system of the trading venue or being likely to do so, including by entering orders which result in the overloading or destabilisation of the order book; or
  - creating or being likely to create a false or misleading signal about the supply of, or demand for, or price of, a financial instrument, in particular by entering orders to initiate or exacerbate a trend (*Article 12(2)(c), MAR*).

In its February 2015 *final report* containing technical advice on possible delegated acts concerning MAR, the European Securities and Markets Authority (ESMA) set out its technical advice on specification of the indicators of market manipulation in Annex I to MAR. The European Commission subsequently adopted a Delegated Regulation supplementing MAR which was based on this (and other) technical advice from ESMA. It was published in the Official Journal of the EU (OJ) in April 2016 as *Commission Delegated Regulation ((EU) 2016/522)* and has applied since 3 July 2016. Annex II

to this Delegated Regulation sets out the indicators of manipulative behaviour for the purposes of sections A and B of Annex I to MAR.

In *issue 56* of the FCA's Market Watch newsletter (dated September 2018) the FCA comments that:

> "We have observed firms referring in market abuse risk assessments to the list of indicators for fictitious devices, false or misleading signals and price securing in MAR (and the list of related practices in the level two legislation [that is, Commission Delegated Regulation *(EU) 2016/522*, Annex II]) and treating those lists as exhaustive. We remind firms that **the lists in MAR are not exhaustive**; firms treating them as such may fail to identify the risk of, and so fail to detect and report, other types of market manipulation which are still within the broader scope of MAR article 12(1)(a) and (b). Similarly, we remind trading venue operators of the **requirement to consider signals not specifically listed in the MiFID II level two legislation** [that is, Commission Delegated Regulation *(EU) 2017/565*, Annex III, section B] when they design surveillance to detect and report possible market abuse." (Our emphasis added.)

In addition, in a November 2017 *speech*, Julia Hoggett made it clear that:

> "It is important to recognise that ignorance of the requirements of MAR, or the absence of intent to commit market abuse, are not a defence to breaches of MAR. Abusive conduct committed in ignorance of the rules can be every bit as serious in its consequences as deliberate, dishonest conduct, and we will pursue it accordingly. Market participants should therefore take all necessary steps to understand their obligations under MAR and ensure that they conduct themselves appropriately."

For more information on the Article 15 MAR market manipulation offence, see *Practice note, Market Abuse Regulation (MAR): overview: Market manipulation*.

Penalties

For breaches of MAR, the FCA can impose unlimited fines, order injunctions and/or prohibit regulated firms or individuals from undertaking regulated activities.

Defences

Article 13 of MAR provides a defence if the transaction or order to trade was "legitimate" and conforms with an AMP on the market concerned. By taking into account the criteria set out in Article 13(2) of MAR, competent authorities can establish AMPs in a market for which they have responsibility for market abuse supervision. ESMA must be notified of the intention to establish an AMP and it will then issue an opinion assessing the compatibility of the AMP with Article 13(2) of MAR.

It is worth noting that a market practice that has been established by a competent authority as an AMP in a particular market will not be considered to be applicable to other markets unless the competent authorities of those other markets have accepted that practice in line with Article 13 of MAR (*Article 13(2), MAR*). In addition, an infringement could still be deemed to have occurred if the competent authority establishes that there was an illegitimate reason behind the relevant transactions or orders to trade (*Recital 42, MAR*).

In the UK, as confirmed on an FCA *webpage* relating to MAR, the FCA has not, to date, established any AMPs under Article 13(2) of MAR.

For more information on AMPs and the process of establishing an AMP, see *Practice note, Market Abuse Regulation (MAR): overview: Accepted market practices (AMPs)*.

FS Act 2012

Offences

Under *section 89* of the FS Act 2012, it is (in summary) an offence for a person to make a statement or to conceal facts with the intention of inducing another person either to:

- Enter into, or to refrain from entering into, a relevant agreement.
- Exercise, or refrain from exercising, any rights conferred by a relevant instrument.

A person commits this offence if they do any of the following:

- Make a statement that they know to be false or misleading in a material respect.
- Make a statement that is false or misleading in a material respect, being reckless as to whether it is.
- Dishonestly conceal any material facts, whether in connection with a statement they make or otherwise.

For more information, see *Practice note, False or misleading statements and impressions: criminal offences and FCA powers: False or misleading statements: section 89 offence*.

Under *section 90* of the FS Act 2012, it is (in summary) an offence for a person to act or engage in a course of conduct that creates a false or misleading impression as to the market in, or the price or value of, any relevant investments. A person commits this offence if they intend to create the impression, and either or both of the following apply:

- The person intends, by creating the impression, to induce another person to acquire, dispose of, subscribe for or underwrite the investments or to refrain from doing so.

- The person knows that the impression is false or misleading or is reckless as to whether it is, and either:
  - intends to produce the results referred to in section 90(4) of the FS Act 2012; or
  - is aware that creating the impression is likely to produce any of the results in that section.

The "results" in section 90(4) of the FS Act 2012 are the making of a gain for the person creating the impression or another person, or the causing of loss to another person, or the exposing of another person to the risk of loss.

For more information, see *Practice note, False or misleading statements and impressions: criminal offences and FCA powers: False or misleading impressions: section 90 offence*.

Penalties

An offence under sections 89 and 90 of the FS Act 2012 carries a maximum punishment of seven years' imprisonment and/or an unlimited fine.

Fraud Act 2006

Offence

Under section 2 of the Fraud Act 2006, it is an offence for a person to dishonestly make a false representation, if they intend, by making the representation, to do either of the following:

- Make a gain for themselves or another.
- Cause loss to another or expose another to a risk of loss.

Following the Supreme Court's recent ruling in *Ivey v Genting Casinos [2017] UKSC 67*, the test for dishonesty is no longer the two-stage *Ghosh* test (which included both objective and subjective elements), but is now a purely objective test, namely: has the accused been dishonest by the standards of an ordinary, reasonable individual (having the same knowledge as the accused)?

For more information on, and an analysis of, the Supreme Court's decision, see *Legal updates, Judging criminal dishonesty no longer involves a subjective test (Supreme Court)*and *Abandoning Ghosh – an important safeguard lost?*.

A "representation" is false if both of the following apply:

- It is untrue or misleading.
- The person making it knows that it is, or might be, untrue or misleading.

A "representation" may be express or implied and may be regarded as made if it is submitted in any form to any system or device designed to receive, convey or respond to communications (with or without human intervention).

For more information, see *Practice note, Fraud by false representation*.

Penalties

An offence under section 2 of the Fraud Act 2006 carries a maximum punishment of seven years' imprisonment and/or an unlimited fine.

Enforcement of spoofing laws by US authorities

Prosecutions of individuals

CFTC v Navinder Singh Sarao

In *CFTC v Navinder Singh Sarao*, point-and-click trader Navinder Singh Sarao was ordered to pay USD38.6 million in penalties and disgorgement after pleading guilty to one count of wire fraud and one count of spoofing on the CME from 2010 to 2014. Mr Sarao is a UK national who the UK courts allowed the US authorities to extradite. During the relevant time period, Mr Sarao traded tens of thousands of E-mini futures contracts in calculated, short time intervals. The CFTC found that Mr Sarao, *"utilized a combination of automated and manual trading systems to place, modify, and cancel orders, resulting in a very high number of orders, modifications, cancelations, and transactions, especially compared to other E-mini S&P market participants."*

Specifically, Mr Sarao placed orders on 6 May 2010 that were modified over 81,000 times, with only 81 lots resulting in executed trades. Mr Sarao's manipulative trading method was alleged to have contributed to the 2010 "flash crash," in which the Dow Jones Industrial Average index dropped 1,000 points, but quickly recovered in 20 minutes. Mr Sarao admitted that he made a profit of USD12.8 million as a result of this scheme. To prove his intent, the government presented evidence of emails between Mr Sarao and a trading platform programmer, discussing the inclusion of the following functions: a *"cancel if close function"*, the ability to *"alternate the closeness (that is, one price away or three prices away)"*, and *"a facility to be able to enter multiple orders at different prices using one click"*.

For more information, see this CFTC *press release* (dated 17 November 2016).

US v Jitesh Thakkar

In March 2019, more than a year after Navinder Sarao pleaded guilty (see *CFTC v Navinder Singh Sarao* above) the trial of Jitesh Thakkar began. Mr Thakkar was the software engineer who created the programme that enabled Mr Sarao's trading and allegedly contributed to the 2010 flash crash.

In January 2018, Mr Thakkar, the owner of Edge Financial Technologies Inc., became the first FinTech software engineer to be charged (in *CFTC v Jitesh Thakkar and Edge Financial Technologies Inc.*) as a co-conspirator for use of technology by another party. There was speculation that, if the government succeeded in convicting Mr Thakkar, it would open the door to future prosecutions against programmers, and specific targeting of the use of "smart contracts" that can be written by programmers directly into the code of a trading programme.

However, the judge dismissed the conspiracy charges mid-trial, allowing the case to continue solely on the spoofing charges. Ultimately, the trial ended in a jury mistrial, with the government deciding not to pursue a retrial. This setback for the DOJ may reverberate beyond *Thakkar*, as it could temper the DOJ's more creative attempts to expand the scope of spoofing liability.

For additional commentary by King & Spalding's Special Matters and Government Investigations team, see *Article, King & Spalding: transatlantic business crime and investigations May column: New developments in spoofing*.

US v Coscia

In August 2017, in *US v Coscia*, the Seventh Circuit upheld the conviction of trader Michael Coscia for spoofing, holding that:

> "The [CEA's] anti-spoofing provision provides clear notice and does not allow for arbitrary enforcement. Consequently, it is not unconstitutionally vague."

The underlying CEA spoofing charges were based on Mr Coscia's calculated trading method in which he used pre-programmed algorithms to execute high-frequency trades in commodities (gold, soybean oil, and high-grade copper) in 2011. To carry out this spoofing scheme, Mr Coscia created artificial market movement by placing small orders of commodities at a price higher (or lower) than the then current sell (or buy) -side market price. He subsequently placed large orders on the opposite side in increasing (or decreasing) price increments to create the illusion that there was price movement. Once the market met his desired buy (or sell) position, he would cancel the orders on the opposite side of the book.

Mr Coscia executed these trading strategies thousands of times, profiting in the amount of USD1.4 million. The Seventh Circuit distinguished legal trading practices involving cancelled orders from spoofing activities also involving cancelled orders, by clarifying that spoofing requires the intent to cancel the order **at the time it was placed**. Conversely, the execution of legal trading practices such as FoK orders and stop-loss orders relies upon the occurrence of certain subsequent events (see *Legal order cancellations* above). The government proved Mr Coscia's intent to cancel using testimony from trading programme designers who stated that he asked that the programmes act "*[l]ike a decoy*," which would be "*[u]sed to pump [the] market*" and that *"large-volume orders were designed specifically to avoid being filled and accordingly would be cancelled in three particular circumstances: (1) based on the passage of time (usually measured in milliseconds); (2) the partial filling of the large orders; and (3) complete filling of the small orders."*

Based on this evidence, the Seventh Circuit affirmed that a rational jury would have found that Mr Coscia intended to cancel the orders before they were executed, violating the anti-spoofing provision of the CEA.

US v Flotron

In April 2018, in *US v Flotron*, a jury in the US District Court for the District of Connecticut acquitted Andre Flotron, a Swiss national and former trader at a global investment bank, of spoofing the precious metals market. Prosecutors charged Mr Flotron on the basis of his pattern of order and trade activity. According to the criminal complaint, his trading pattern entailed placing small trades that were capable of execution (primary orders) on one side of the market close to the prevailing price. Then, either before or after placement of the primary order, Mr Flotron allegedly placed a larger order on the opposite side of the market from the primary order (opposite order) that was at least ten times as large as the size of the primary order and close to the prevailing price. When at least one of the primary orders was filled, Mr Flotron would immediately cancel his opposite order (at most no more than five seconds after placing the opposite order and, in any event, before it could be executed).

Although the government presented evidence of trading data and testimony from Mr Flotron's two former colleagues, who claimed that he taught them how to spoof and that it was commonplace in the industry, the jury was did not find that he possessed the requisite intent to cancel his orders at the time they were placed and returned a verdict of not guilty.

US v Gandhi and US v Mohan

In November 2018, the DOJ announced guilty pleas entered into by two commodities traders for commodities fraud and spoofing conspiracy, in *US v Gandhi* and *US v Mohan*.

Mr Gandhi and Mr Mohan admitted that, from March 2012 to March 2014, they conspired with fellow trader Yuchun "Bruce" Mao and others at their trading firm to mislead the markets for E-Mini S&P 500 and E-Mini NASDAQ 100 futures contracts traded on CME, as well as E-Mini Dow futures contracts traded on the Chicago Board of Trade (CBOT). In addition, the ex-traders admitted that they and their co-conspirators placed thousands of orders that they did not intend to execute, in order to obtain executions of other orders at better prices, quantities, and times. The scheme resulted in market losses of more than USD60 million.

Further, Mr Gandhi admitted that, from May 2014 to October 2014, while employed at a different trading firm, he conspired with others to mislead the markets for E-Mini S&P 500 futures contracts traded on the CME by agreeing to place, and placing, hundreds of spoof orders for E-Mini S&P 500 futures contracts, to create the false and misleading appearance of increased supply or demand. The scheme resulted in market losses of more than USD1.3 million. Both Mr Gandhi and Mr Mohan are awaiting sentencing.

For more information, see this DOJ *press release* (dated 6 November 2018).

Mr Gandhi and Mr Mohan separately settled charges with the CFTC, admitting engaging in manipulative and deceptive schemes that involved thousands of acts of spoofing.

For more information, see this CFTC *press release* (dated 12 October 2018) and this CFTC *press release* (dated 25 February 2019).

Failure to supervise

In January 2017, the CFTC filed and settled its first "failure to supervise" case against a registered firm related to spoofing. Under CFTC Regulation 166.3, firms must employ diligent supervision of its employees and activities, and case law has interpreted this duty of diligence broadly.

In January 2018, the CFTC filed eight anti-spoofing enforcement actions against three entities, and ultimately settled supervisory violations as part of that action.

For more information, see this CFTC *press release* (dated 19 January 2017) and this CFTC *press release* (dated 29 January 2018).

First CFTC spoofing non-prosecution agreement

The CFTC entered into its first NPA for a spoofing offence in June 2017. The CFTC entered into the NPA with three former traders employed by a global investment bank after observing large "book imbalances" in their company's trades and finding that the traders had engaged in spoofing on at least 80 occasions by:

- Placing large orders on the opposite side of the market from smaller orders.
- Quickly cancelling the large orders within seconds after either the smaller resting orders had been filled or the traders believed that the spoofing orders were at too great a risk of being executed.

Additionally, the CFTC fined the company USD25 million in civil penalties for failure to supervise.

For more information, see this CFTC *press release* (dated 29 June 2017).

CFTC spoofing orders

Victory Asset Inc.

In September 2018, the CFTC issued orders against Victory Asset Inc. and its trader Michael Franko for spoofing (in violation of CEA Sections 4c(a)(5) and 6(c)(1)). The administrative settlements in *In re Michael D. Franko* and *In re Victory Asset Inc.* arose from Mr Franko's cross-market spoofing that sought to take advantage of the correlation between prices of copper future contracts on US and UK exchanges. Victory and Mr Franko were ordered to pay civil monetary penalties of USD1.8 million and USD500,000 respectively, with Mr Franko further banned from trading in US futures markets for a period of six months.

For more information, see this CFTC *press release* (dated 19 September 2018).

Mizuho Bank Ltd

In *In re Mizuho Bank Ltd*, the CFTC alleged that a Singapore-based interest rates trader violated CEA Section 4c(a)(5) by placing large orders and then cancelling them within seconds. However, the CFTC did not allege that any trader placed or executed a genuine order meant to benefit from the illicit order. Rather, the CFTC alleged that the trader *"placed these spoof orders to test market reaction to [the trader's] trading in anticipation of having to hedge Mizuho swaps positions with futures at a later date."* Mizuho was ordered to pay a civil fine of USD250,000.

Mizuho is the first civil or criminal CFTC spoofing action in which the CFTC took advantage of the court's articulation in *Coscia* (see *US v Coscia* above) regarding the elements of CEA Section 4c(a)(5), by solely alleging a spoof order without a corresponding primary order meant to benefit from the spoof.

For more information, see this CFTC *press release* (dated 21 September 2018).

Bank of Nova Scotia

In October 2018, the CFTC issued an *order* filing and settling charges against the Bank of Nova Scotia (BNS) for engaging in multiple acts of spoofing in gold and silver futures contracts traded on the CME. The order found that BNS engaged in this activity by and through traders on its precious metals trading desk from at least June 2013 to June 2016. The order required BNS to pay a USD800,000 civil monetary penalty. This matter involved notification of the misconduct by BNS' Futures Commission Merchant, and when BNS became aware of the misconduct, BNS self-reported the conduct to the CFTC.

For more information, see this CFTC *press release* (dated 1 October 2018).

SEC and FINRA Enforcement Actions

Lek Securities Corporation, et al.

In March 2017, the SEC and FINRA filed related enforcement actions against broker-dealer Lek Securities Corporation and Avalon FA Ltd, a Ukraine-based unregistered trading firm, accusing Avalon of manipulating the US securities markets by engaging in layering, spoofing, and cross-market manipulation through Lek Securities' direct market access platform. The SEC alleged that Avalon, through Lek Securities, generated more than USD28 million in illicit profits. After filing its *complaint* in the US District Court, Southern District of New York, the SEC obtained an emergency order freezing Avalon's assets held in its account at Lek Securities, as well as freezing and repatriating funds that Avalon had transferred overseas. The enforcement action, which is pending, seeks civil penalties and disgorgement of "*all ill-gotten gains as a result of [the defendants'] unlawful conduct*."

FINRA, through its Department of Market Regulation, brought an independent action against Lek Securities and its CEO, Samuel F. Lek, charging them with aiding and abetting Avalon's fraud, and violating FINRA rules concerning market access and supervision. FINRA also filed related actions on behalf of several exchanges, including the NYSE and Nasdaq. In its pending *complaint*, FINRA requests that its administrative tribunal make findings that, if sustained, would result in the statutory disqualification of Lek Securities.

For more information, see this SEC *press release* (dated 10 March 2017) and this FINRA *press release* (both dated 27 March 2017).

Enforcement of spoofing laws by UK authorities

As noted above (see *Offences and enforcement framework: UK*), to date, the FCA (formerly the FSA) has only pursued civil spoofing cases under section 118(5) of FSMA (repealed with effect from 3 July 2016, the application date of *MAR*). The sections below highlight FCA and FSA enforcement action in relation to the former section 118(5) FSMA manipulating transactions offence.

For more information, see *Practice note, Market abuse: the types of behaviour (pre-MAR regime): Manipulating transactions: examples of FCA and FSA enforcement action*.

FCA: final notice to Michael Coscia

In July 2013, the FCA issued a *final notice* to Michael Coscia, fining him £597,993 for layering thousands of futures orders on ICE Futures Europe (ICE) in violation of section 118(5) of FSMA. Specifically, the FCA found that over a period of six weeks and using high frequency trading, Mr Coscia placed large orders in the order book for less than one second, after which the orders (small or large) were cancelled immediately and simultaneously if not previously executed. The FCA concluded that Mr Coscia's trading activity created a misleading impression on the market as his large cancelled orders created false impressions of liquidity and caused at least one significant market participant to withdraw from ICE.

For more information, see *Legal update, FCA fines US based high frequency trader US$903,176 for deliberate manipulation of commodities markets*.

Issue 44 of the FCA's Market Watch newsletter (dated August 2013) includes an article on this FCA enforcement action.

FCA: final notice to Paul Walter

In November 2017, the FCA issued a *final notice* to Paul Walter, fining him £60,090 for engaging in market abuse in violation of section 118(5) of FSMA. The FCA found that Mr Walter was able to manipulate the market 12 times. Specifically, Mr Walter entered high bid quotes on the BrokerTec trading platform for a Dutch State Loan (DSL). Once he saw that other market participants raised their own bids in response to his high bids, he cancelled his own quotes and sold each DSL to other market participants for a higher price.

Despite the FCA's conclusion that Mr Walter was negligent, rather than deliberate, it found that Mr Walter engaged in market abuse. The FCA reasoned that his repeated trading strategy negatively affected other market participants by giving them a false and misleading impression as to the price and supply or demand of the DSLs and secured prices at an artificial level.

For more information, see *Legal update, FCA fines former bond trader for market abuse*.

FCA v Swift Trade

In December 2013, in *7722656 Canada Inc and another v FCA [2013] EWCA Civ 1662*, the Court of Appeal upheld an Upper Tribunal (Tax and Chancery Chamber) decision that the appellant, Canada Inc (a Canadian company formed following the amalgamation of Swift Trade Inc and another Canadian company) engaged in market abuse in breach of section 118(5) of FSMA.

The FSA had proposed fining Swift Trade £8 million, having found that individual traders engaged in market manipulation by repeatedly layering thousands of orders for contracts for differences (see *Legal update, FSA proposes to fine Swift Trade Inc £8 million for market abuse*). Specifically, the defendants' trading activity involved placing on the order book a series of short-lived (and large) orders to buy or sell shares that were close to the touch price. Once the defendants placed those large orders, it gave the impression of substantial demand for, or supply of, the shares. As a result, this caused the share price to move up (for bids) or down (for offers), such that the smaller orders that were entered by Swift Trade on the other side of the order book became more attractive and were executed. The FSA concluded that the defendants' layering activity created a distinct, artificial movement of the price from which the defendants reaped a benefit to the detriment of the other market participants. Accordingly, the defendants engaged in market manipulation by impacting the market through distorting the price formation process and by misrepresenting the overall liquidity on the order book for the shares in question.

Following the Court of Appeal's judgment, the FCA went on to impose the £8 million fine (see *Legal update, FCA fines Swift Trade for market abuse*).

FCA v Da Vinci Invest

In August 2015, in *FCA v Da Vinci Invest Ltd [2015] EWHC 2401 (Ch)*, the High Court affirmed the FCA's £7,570,000 penalty against individual traders and Da Vinci Invest Ltd for their layering behaviour in violation of section 118(5) of FSMA.

Using algorithmic trading, the traders repeatedly placed a series of orders on the London Stock Exchange (LSE) and immediately and automatically placed directly corresponding orders to move the price of the shares. The traders subsequently took advantage of the price by buying and selling, then cancelling the opposite orders.

The FCA presented expert testimony that the *"[t]raders' placing of numerous orders on one side of the order book gave, or was likely to have given, other market participants the impression of an increased supply or demand for the shares in question."* The High Court analysed the distinct pattern and *"level of passive and cancelled orders, the numbers of wash-trades and the examples of buying high and selling low"*, which were repeated several times over the relevant periods, and concluded that this trading activity effected a false or misleading impression as it was too similar and too frequent to be the result of coincidence or some other innocent strategy.

The High Court concluded that the traders' layering behaviour constituted market abuse because it was, *"intended to cause a movement in the market price of the share in question and to induce other market participants to place similar larger orders, with which the traders could then trade aggressively in the opposite direction."* Specifically, *"these orders had the effect of moving the share price as the market adjusted to the apparent shift in the balance of supply and demand. Once the price had been moved to an advantageous level, the defendants initiated a trade on the other side of the order book in order to profit from the price movement that they had created."*

In this case, the High Court emphasised that a violation of section 118(5) of FSMA focused on *"the likely perception of other parties, not the state of mind of the person whose behaviour is under consideration."* Therefore, market abuse in this context did not *"require a showing of the mental element on the part of the person or persons alleged to have engaged in market abuse."*

For more information, see *Legal update, High Court grants FCA permanent injunction and penalties against companies and individuals for committing market abuse*.

Key points on US and UK spoofing enforcement

Both manual and high frequency, algorithmic trading methods have been the subject of spoofing enforcement. Although regulators more commonly focus on large spoofing orders, they have analysed small orders as well: a single cancelled order may be scrutinised and form the basis of an offence.

Based on previous cases (see *Enforcement of spoofing laws by US authorities* and *Enforcement of spoofing laws by UK authorities* above), US and UK enforcement authorities have scrutinised the following trading activity to determine whether behaviour constitutes market manipulation:

- The size discrepancy between buy and sell orders on both sides of the market (*Swift Trade*).
- The number of times orders were modified (*Sarao*).
- The percentage of cancelled or filled orders relative to the total number of orders placed (*Coscia, Flotron*).
- Placing multiple orders at different price levels and cancelling them before they are filled (*Sarao*).
- The pattern of the order and trade activity (*Flotron, Walter*).
- The high proportion of the traders' orders in relation to the shares in question (*Da Vinci*).
- The passage of time before large volume orders were cancelled (*Coscia, Da Vinci*).
- The frequency of the order patterns (*Da Vinci, Swift Trade*).
- Large book imbalances in a company's trades (first CFTC NPA).
- The length of time the orders remained on the order book (*Swift Trade*).

Enforcement authorities in both the US and the UK use data from an individual's trading patterns as the basis for their enforcement actions. However, trading patterns that include cancellation strategies may be entirely legitimate.

US

In the US, when distinguishing between legitimate trading and spoofing, the government must prove that the trader had the specific intent (or at least "beyond reckless" in a civil case) to cancel the order at the time it was placed. To prove intent in spoofing cases, the government has offered evidence of contemporaneous communication and witness testimony. Based on the enforcement actions and cases to date, the determination of whether a trading practice constitutes spoofing in the US hinges on evidence surrounding the trader's intent in addition to an analysis of relevant trading data. Additionally, corporations can be charged with failure to supervise spoofing if a trader allegedly engages in spoofing, even where the underlying violation remains unproved.

UK

In the UK, based on limited existing cases and regulatory action under previous law, liability for spoofing appears to hinge on analysing the trading activity's effect on the market and whether the trading activity that utilised cancellations created a false or misleading impression. The prosecutor does not necessarily need to prove that the trader specifically intended to create a false or misleading impression. Therefore, in the UK, traders who use cancellation techniques can potentially be held liable for civil market abuse without having any wrongful intent, and may theoretically incur criminal liability despite having engaged in only negligent or reckless conduct.