Milbank

Global Litigation & Arbitration Group

US & UK Litigation Briefing

SPOOFING UNDER US AND UK LAW

21 June 2021

Key Contacts

James Cavoli
Partner
+1 212.530.5172
jcavoli@milbank.com

William Charles
Partner
+44 20.7615.3076
wcharles@milbank.com

Charles Evans
Partner
+44 20.7615.3090
cevans@milbank.com

Emily Clarke
Law Clerk
+1 212.530.5036
eclarke@milbank.com

Kayla Giampaolo
Associate
+1 212.530.5217
kgiampaolo@milbank.com

Conrad Marinkovic
Associate
+44 20.7615.3085
cmarinkovic@milbank.com

On May 24, 2021, Milbank's White Collar Defense and Investigations Group announced the publication of "*A Practice Guide on the Law of Spoofing in the Derivatives and Securities Markets*," a whitepaper published by Wolters Kluwer Legal and Regulatory US.[1] This Guide provides a detailed analysis of the statutory frameworks used to combat spoofing—a form of price manipulation—in the US and a comprehensive treatment of key US case law developments, spoofing enforcement actions and private litigation.

In the UK, spoofing and related forms of market manipulation have been a focus for the regulatory authorities for some time. Most recently, on May 28, 2021, the Financial Conduct Authority ("**FCA**") published a Market Watch newsletter which focuses on the FCA's efforts to identify market manipulation (including spoofing) and recent enforcement activity in this regard.[2]

In this article, we examine the prevailing regimes concerning spoofing in the US and UK, including the key similarities and differences between them.

Spoofing: the US regime

Although regulators in the US have long asserted that what we now call spoofing—bidding or offering with the intent to cancel the bid or offer before execution—undermines the integrity of the markets, it was not

---

[1] Available at https://www.milbank.com/en/news/milbank-publishes-a-practice-guide-on-the-law-of-spoofing-in-the-derivatives-and-securities-markets.html.
[2] Available at https://www.fca.org.uk/publications/newsletters/market-watch-67.

until the passage of the 2010 Dodd-Frank Wall Street Reform and Consumer Protection Act ("**Dodd-Frank**") that such conduct was outlawed by name in relation to the trading of commodities and derivatives.

The Department of Justice ("**DOJ**") has become more active in prosecuting spoofing since Dodd-Frank's anti-spoofing provision became effective in 2011, having commenced a total of 15 criminal cases against 20 individuals for derivatives spoofing since that time (actions against 16 of the 20 individuals were commenced in or after 2018). On the civil side, the Commodities Futures Trading Commission ("**CFTC**") has commenced a total of 61 spoofing enforcement actions since Dodd-Frank. As described in more detail below, this greater focus on spoofing has led to creative charging decisions by the DOJ and resulted in various judicial decisions that have made spoofing easier to prosecute.

The DOJ has been less active with respect to securities markets, as to which Dodd-Frank does not apply, having prosecuted only four individuals for securities spoofing since 2011. For its part, the Securities Exchange Commission ("**SEC**") has commenced a total of 13 civil enforcement actions for securities spoofing during that same period.

The US criminal regime

(i) Legal framework

Prior to the passage of Dodd-Frank, the DOJ had the ability to pursue criminal spoofing charges under various Title 18 statutes, including the wire fraud statute, 18 U.S.C. § 1343, and the commodities fraud statute, 18 U.S.C. § 1348.[3] Despite the availability of these statutes, the DOJ never used them to prosecute spoofing activity pre-Dodd-Frank.

As part of Dodd-Frank, the Commodities Exchange Act ("**CEA**") was amended in several ways that expanded the DOJ's ability to combat spoofing. The DOJ can prosecute spoofing under the following provisions of the CEA:

- CEA § 4c(a)(5)(C) is the specific anti-spoofing provision. This provision prohibits "*any trading, practice, or conduct on or subject to the rules of a registered entity that…is of the character of, or is commonly known to the trade as 'spoofing' (bidding or offering with the intent to cancel the bid or offer before execution).*" 7 U.S.C. § 6c(a)(5).
- CEA § 6(c)(1) is a securities-style anti-manipulation provision modeled after § 10(b) of the Securities Exchange Act of 1934 ("**Exchange Act**"). This provision makes it "*unlawful for any person, directly or indirectly, to use or employ, or attempt to use or employ, in connection with any swap, or a contract of sale of any commodity in interstate commerce, or for future delivery on or subject to the rules of any registered entity, any manipulative or deceptive device or contrivance, in a contravention of such rules and regulations as the Commission shall promulgate*." 7 U.S.C. § 9(1) (2012).
- CEA § 6(c)(3) is an updated version of one of the CEA's pre-Dodd-Frank anti-manipulation provisions. This provision makes it "*unlawful for any person, directly or indirectly, to manipulate or attempt to manipulate the price of*" a swap, commodity, or future. 7 U.S.C. § 9(3).
- CEA § 9(a)(2), which existed prior to, and was not amended by, Dodd-Frank, makes it unlawful *"for* [a]*ny person to manipulate or attempt to manipulate the price of any commodity in interstate commerce, or for future delivery on or subject to the rules of any registered entity, or of any swap . . .*" 7 U.S.C. § 13(a)(2).

[3] Prior to the 2009 passage of the Fraud Enforcement and Recovery Act, Pub. L. No. 111-21, 123 Stat. 1617 (2009), 18 U.S.C. § 1348 prohibited only securities fraud. It now prohibits both securities fraud and commodities fraud. *See* 18 U.S.C. § 1348 (2012).

The DOJ can bring criminal cases for "knowing" violations of the above provisions of the CEA, each of which has a five-year limitation period.[4] If convicted, an individual defendant faces a statutory maximum of ten years' imprisonment and a $1 million fine.[5]

Since the enactment of Dodd-Frank, the DOJ has invoked the specific anti-spoofing provision, as well as other provisions of the CEA, to combat spoofing. But it has not stopped there. The DOJ has also begun to use the wire and commodities fraud statutes to prosecute spoofing cases.[6] Courts have affirmed—after significant challenges by defendants—that spoofing can constitute a "*scheme to defraud*" within the meaning of these Title 18 statutes.[7] The DOJ has also recently prosecuted spoofing conduct as bank fraud under 18 U.S.C. § 1344 and RICO conspiracy under 18 U.S.C. § 1962(d).[8] Challenges to the application of those statutes to spoofing conduct are currently pending.

(ii) *Current practice*

After Dodd-Frank, the DOJ was slow to start prosecuting individuals or organizations under the new anti-spoofing provision. From 2011 to 2017, the DOJ only charged four individuals for spoofing in relation to futures contracts. The first such charge was in 2014 against Michael Coscia, the then-owner of Partner Energy Trading LLC, a high frequency trading company.[9] Mr Coscia went to trial and was convicted on all counts in 2015.[10]

In 2018 and 2019, the DOJ quadrupled its efforts, charging 16 individuals for criminal spoofing violations in relation to futures contracts.[11] Of the 20 individuals charged since 2011, eight have pled guilty (often

---

[4] 7 U.S.C. § 13(a)(2); 18 U.S.C. § 3282.

[5] 7 U.S.C. § 13(a)(2).

[6] *See, e.g., United States v. Bases*, No. 18-Cr-00048 (N.D. Ill.); *United States v. Vorley*, No. 18-Cr-00035 (N.D. Ill.); *United States v. Coscia*, No. 14-Cr-00551 (N.D. Ill.).

[7] *See United States v. Coscia*, 866 F.3d 782 (7th Cir. 2017); Order, *United States v. Vorley*, No. 18-cr-00035 (N.D. Ill. Jul. 21, 2020), ECF No. 254.

[8] *See United States v. Smith*, 19-Cr-00669 (N.D. Ill.).

[9] *Coscia*, No. 14-Cr-00551 (N.D. Ill. Oct. 1, 2014) (indictment filed). *See also* the FCA Final Notice dated 3 July 2013 in relation to Mr Coscia (available at https://www.fca.org.uk/publication/final-notices/coscia.pdf) (as summarised in the Appendix).

[10] *Id.*; Greg Trotter, *Trader Michael Coscia 1st in nation to be sentenced under 'anti-spoofing' law,* CHICAGO TRIBUNE (July 13, 2016), https://www.chicagotribune.com/business/ct-spoofing-trial-sentencing-0714-biz-20160713-story.html.

[11] In addition to Mr Coscia, *see United States v. Smith*, No. 19-Cr-669 (N.D. Ill. Aug. 22, 2019) (indictment filed; superseding indictment filed on Nov. 14, 2019); *United States v. Trunz*, No. 19-Cr-00375 (E.D.N.Y. Aug. 20, 2019) (information filed); *United States v. Flaum*, No. 19-Cr-338 (E.D.N.Y. July 25, 2019) (information filed); *United States v. Edmonds*, No. 18-Cr-239 (D. Conn. Oct. 9, 2018) (information filed); *United States v. Gandhi*, No. 18-Cr-609 (S.D. Tex. Oct. 11, 2018) (information filed); *United States v. Mohan*, No. 418-Cr-00610 (S.D. Tex. Oct. 11, 2018) (information filed); *United States v. Mao*, No. 18-Cr-00606 (S.D. Tex. Oct. 10, 2018) (indictment filed); *United States v. Thakkar*, No. 18-Cr-00036 (N.D. Ill. Feb. 14, 2018) (indictment filed); *United States v. Vorley*, No. 18-Cr-00035 (N.D. Ill. Jan. 19, 2018) (complaint filed; indictment filed July 24, 2018); *United States v. Bases*, No. 18-Cr-00048, (N.D. Ill. Jan. 25, 2018) (complaint filed; indicted on July 18, 2018); *United States v. Flotron*, No. 17-Cr-00220 (D. Conn. Sept. 26, 2017) (indictment filed; superseding indictment filed on Jan. 30, 2018); *United States v. Zhao*, No. 28-Cr-00024 (N.D. Ill. Jan. 11, 2018 (complaint filed; information filed on Dec. 18, 2018); *United States v. Liew*, No. 17-Cr-00001 (N.D. Ill. Jan. 3, 2017) (criminal complaint filed; information filed on May 24, 2017); *United States v. Sarao*, No. 15-Cr-00075 (N.D. Ill. Feb. 11, 2015) (criminal complaint filed; informed filed on Sept. 2, 2015).

agreeing to cooperate with the government);[12] three went to trial and were convicted;[13] two went to trial and were exonerated;[14] one is a fugitive;[15] and six have pled not guilty and are at various stages of pretrial proceedings.[16] Three of the individuals who pled guilty or were convicted have been sentenced. The two individuals who pled guilty received sentences of time-served (one for 120 days and the other for 302 days),[17] while Mr. Coscia, who was convicted after trial, was sentenced to three years' imprisonment and two years of supervised release.[18] None of the three sentenced individuals were assessed criminal fines, but one was required to forfeit $12.9 million in criminal proceeds.[19]

The DOJ has also ramped up its prosecution of organizations for spoofing violations in recent years (nearly all in relation to futures contracts). Since 2019, five organizations have entered into deferred prosecution agreements ("**DPAs**") or non-prosecution agreements ("**NPAs**") with the DOJ, with monetary sanctions ranging from $1 million to $920.2 million.[20]

The DOJ also prosecutes individuals and organizations for spoofing in relation to securities trading, though it has been much less active in this space relative to the futures markets. Since 2011, the DOJ has proceeded against four individuals and one organization.[21] The individuals were charged with conspiracy to commit securities fraud in violation of 18 U.S.C. §§ 371 and/or 1349; securities fraud in violation of 18 U.S.C. § 1348; and/or securities fraud in violation of § 10(b) of the Exchange Act, 15 U.S.C. § 78j(b). Two of the four individuals pled guilty and were sentenced—one was sentenced to five years' probation and a $10,000 fine,[22] and the other was sentenced to 18 months' imprisonment and one year of supervised release.[23] The criminal charges against the remaining two individuals are pending. The organization entered into one of the DPAs discussed above since it committed spoofing violations in both the securities *and* futures markets.

---

[12] Defendants Flaum, Trunz, Gandhi, Mohan, Edmonds, Sarao, Zhao, and Liew pled guilty. *Flaum*, No. 19-Cr-338 (E.D.N.Y. Julu 25, 2019); *Trunz*, No. 19-Cr-00375 (E.D.N.Y. Aug. 20, 2019); *Gandhi*, No. 18-Cr-609 (S.D. Tex. Nov. 2, 2018); *Mohan*, No. 418-Cr-00610 (S.D. Tex. Nov. 6, 2018); *Edmonds*, No. 18-Cr-239 (D. Conn. Oct. 9, 2018); *Sarao*, No. 15-Cr-00075 (N.D. Ill. Nov. 9, 2016); *Zhao*, No. 28-Cr-00024 (N.D. Ill. Dec. 26, 2018); *Liew*, No. 17-Cr-00001 (N.D. Ill. June 1, 2017).

[13] Mr Coscia was convicted in 2015. *See* Coscia, No. 14-Cr-00551 (N.D. Ill.). In September 2020, Messrs Vorley and Chanu were convicted (though not on all counts) of wire fraud in connection with spoofing in relation to precious metals futures. *See United States v. Vorley*, No. 18-Cr-00035 (N.D. Ill.).

[14] Andre Flotron was acquitted by a Connecticut jury in May 2018. *See United States v. Flotron*, No. 17-Cr-00220 (D. Conn.). Jitesh Thakkar was fully exonerated as a result of the district court's judgment of acquittal on one count and the government's decision to dismiss the remaining charges with prejudice after a hung jury. *United States v. Thakkar*, No. 18-Cr-00036 (N.D. Ill.).

[15] The only docket entries in *United States v. Mao*, No. 18-Cr-00606 (S.D. Tex.), indicate that Mr Mao, a Chinese national, was indicted on Oct. 10, 2018, at which time a bench warrant for his arrest was issued.

[16] Defendants Smith, Nowak, Ruffo, Jordan, Bases, and Pacilio pled not guilty and are litigating their cases. *See United States v. Smith*, No. 19-Cr-669 (N.D. Ill.); *United States v. Bases*, No. 18-Cr-00048 (N.D. Ill.)

[17] *See United States v. Sarao*, No. 15-Cr-00075 (N.D. Ill. Sept. 2, 2015); *United States v. Zhao*, No. 18-Cr-00024 (N.D. Ill. Dec. 18, 2018).

[18] *See* Judgment in a Criminal Case, *United States v. Coscia*, No. 14-Cr-00551 (N.D. Ill. July 14, 2016), ECF No. 159.

[19] *See* Judgment in a Criminal Case, *United States v. Sarao*, No. 15-Cr-00075 (N.D. Ill. Jan. 29, 2020), ECF No. 119.

[20] The DOJ entered into DPAs with JPMorgan Chase & Co., Bank of Nova Scotia, Propex Derivatives Pty Ltd, and Tower Research Capital LLC, and a NPA with Merrill Lynch Commodities, Inc.

[21] *See United States v. Wang*, No. 19-Cr-6485 (D. Mass. Oct. 14, 2019) (complaint filed); *United States v. Taub*, No. 16-Cr-8190 (D.N.J. Feb. 21, 2018) (indictment filed); *United States v. Milrud*, No. 15-Cr-455 (D.N.J. Sept. 1, 2015) (information filed).

[22] *See* Judgment in a Criminal Case, *United States v. Milrud*, No. 15-Cr-00455 (D.N.J. Apr. 24, 2020), ECF No. 45.

[23] *See* Judgment in a Criminal Case, *United States v. Taub*, No. 18-Cr-00079 (D.N.J. Dec. 22, 2020), ECF No. 61.

The US civil/regulatory regime

(i) CFTC legal framework

The CFTC is responsible for the civil enforcement of the CEA. Before Dodd-Frank, CEA §§ 6(c) and 9(a)(2) were the primary enforcement mechanisms used by the CFTC to police spoofing. Under CEA § 6(c), the CFTC had the power to bring an administrative enforcement action against traders who, among other things, "*manipulat*[ed] *or attempt*[ed] *to manipulate…the market price*" of commodities or commodities futures contracts. 7 U.S.C. § 9 (2009). CEA § 9(a)(2)—a criminal provision of the statute that was civilly enforceable by the CFTC—made it unlawful to "*manipulate or attempt to manipulate the price*" of commodities or commodities futures contracts. 7 U.S.C. § 13(a)(2) (2009). Given the requisite elements, it was difficult for the CFTC to prove manipulation under these pre-Dodd-Frank provisions.[24] In fact, the CFTC successfully litigated only one contested spoofing matter to final judgment prior to Dodd-Frank.[25]

Dodd-Frank amended the CEA in several ways relevant to spoofing. The following provisions are the primary mechanisms by which the CFTC currently combats spoofing by way of civil enforcement action:

- CEA § 4c(a)(5)(C) is the CEA's specific anti-spoofing provision. 7 U.S.C. § 6c(a)(5). As noted, the DOJ can use this provision to bring criminal actions against individuals and organizations. The CFTC also has the power to enforce this provision in civil enforcement actions.[26] The CFTC has provided "*four non-exclusive examples of possible situations*" that may amount to spoofing in the civil context. These include:
  - "*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*"; and
  - "*Submitting or cancelling bids or offers with intent to create artificial price movements upwards or downwards*."[27]
- Dodd-Frank also added a securities-style anti-manipulation provision, which is in addition to CEA § 6(c)'s pre-existing anti-manipulation provision (described above at page 2). *See* CEA § 6(c)(1), 7 U.S.C. § 9(1) (2012). Like the anti-spoofing provision, CEA § 6(c)(1) can be enforced civilly by the CFTC or criminally by the DOJ.
- CEA § 6(c)(3) incorporates the old four-part price manipulation test from cases that arose under pre-Dodd-Frank §§ 6(c) and 9(a)(2). Like the anti-spoofing provision and CEA § 6(c)(1), CEA § 6(c)(3) can be enforced civilly by the CFTC or criminally by the DOJ.
- The CEA's other anti-manipulation provision, § 9(a)(2), 7 U.S.C. § 13(a)(2), which was not modified by Dodd-Frank, can also form the basis of civil spoofing charges by the CFTC.

---

[24] To prove manipulation under the CEA prior to Dodd-Frank, the government was required to establish that (1) the accused had the ability to influence market prices; (2) he or she specifically intended to do so; (3) artificial prices existed; and (4) the accused caused the artificial prices. *See, e.g., In re Amaranth Natural Gas Commodities Litig.,* 730 F.3d 170, 173 (2d Cir. 2013).

[25] *In the Matter of Anthony J. DiPlacido,* CFTC No. 01-23, 2008 WL 4821204 (Nov. 5, 2008).

[26] The CFTC can bring either an administrative proceeding or district court action for alleged violations of the specific anti-spoofing provision pursuant to CEA § 6c (district court actions) and CEA §§ 6(c), 6(d), 8a (administrative proceedings). The statute of limitations for both district court and administrative enforcement actions is five years. *See* 28 U.S.C. § 2462.

[27] *See* CFTC, *Antidisruptive Practices Authority,* 78 Fed. Reg. at 31892 (May 28, 2013).

The CFTC can pursue civil enforcement of the above-noted statutory provisions either by way of administrative action or district court proceedings.[28]

(ii) *CFTC current practice*

Like the DOJ, the CFTC has been active in spoofing enforcement in recent years. Since 2011, the CFTC has brought 61 cases against a total of 79 defendants. Of the 61 cases, 51 were administrative proceedings and 10 were filed in federal district court. Of the 79 defendants, 36 were individuals and 43 were organizations.

Of the 79 defendants, 70 settled their cases short of trial. Charges are pending against the remaining defendants. A number of the CFTC's civil enforcement actions are stayed pending the outcome of parallel criminal cases.

Defendants found liable in an administrative action for manipulation or attempted manipulation under CEA §§ 6(c)(1) or 6(c)(3) can be barred from trading on an exchange, have their CFTC registrations suspended or revoked, and be forced to pay a penalty or restitution. The penalty for manipulation may not exceed the greater of $1 million or triple the monetary gain to the person for each violation.[29] A violator also may be ordered to cease and desist all unlawful conduct.[30] Defendants found liable for manipulation or attempted manipulation in district court can be subject to an injunction, forced to pay disgorgement, restitution, and a penalty. The maximum penalty is the same as administrative proceedings.[31]

Defendants found liable in an administrative action under the CEA's anti-spoofing provision can also be barred from trading on an exchange, have their CFTC registrations revoked, and be forced to pay a monetary penalty or restitution. The penalty may not exceed the greater of $140,000 or triple the monetary gain to the person for each violation.[32] The violator may also be ordered to cease and desist any future similar conduct.[33] A person found civilly liable for spoofing in a district court proceeding can be subject to an injunction, and be forced to pay disgorgement, restitution, and/or a civil monetary penalty. The maximum penalty is the same as in administrative proceedings.[34]

In the CFTC enforcement actions brought against individuals since 2011, the monetary penalties have ranged from $100,000 to $38.6 million, with an average of approximately $2.4 million per individual and a median of $425,000. In CFTC enforcement actions brought against organizations, the monetary penalties have ranged from $73,600 to $920.2 million, with an average of approximately $31.0 million per organization and a median of $1.5 million.

For conduct occurring on or after July 15, 2011, the CFTC has charged nearly all defendants with spoofing in violation of CEA § 4c(a)(5)(C), 7 U.S.C. § 6c(a)(5)(C). Fewer, but still a substantial number of defendants, were charged with violating CEA §§ 6(c)(1), 6(c)(3) and 9(a)(2) (all described above).

(iii) *SEC legal framework*

Unlike the CEA, the securities statutes do not prohibit spoofing by name. As such, the SEC has taken aim at spoofing related to securities in civil (administrative or district court) actions under more general anti-

---

[28] Both the CFTC and SEC have the authority to decide whether to bring an action in federal district court or before an administrative law judge. Administrative cases are typically faster and less expensive for agencies to litigate as compared to cases in district court.

[29] *See* 7 U.S.C. § 9(10)(C)(ii).

[30] *See* CEA §§ 6(c)(4), 6(c)(10), 6(d), 7 U.S.C. §§ 9(4), 9(10), 13b.

[31] *See* 7 U.S.C. § 13a-1(d)(1)(B).

[32] 7 U.S.C. § 9(10)(C)(i).

[33] *See* CEA §§ 6(c)(4), 6(c)(10), 6(d), 7 U.S.C. §§ 9(4), 9(10), 13b.

[34] *See* CEA § 6c, 7 U.S.C. § 13a-1.

fraud and anti-manipulation statutes. Such cases typically proceed under §§ 9(a)(2) and 10(b) of the Exchange Act[35] and § 17(a) of the Securities Act of 1933 (the "**Securities Act**").[36]

- Section 10(b) of the Exchange Act prohibits "*manipulative or deceptive device*[s] *or contrivance*[s]" in violation of SEC rules such as Rule 10b-5. As the Supreme Court has noted, "*manipulation*" under § 10(b) is a "*term of art when used in connection with securities markets*."[37] It "*connotes intentional or willful conduct designed to deceive or defraud investors by controlling or artificially affecting the price of securities.*"[38] To the extent that spoofing artificially affects securities' pricing or deceives market participants, it may amount to a violation of Section 10(b) and Rule 10b-5. The same holds true with respect to Securities Act § 17(a) since the elements are, in large part, the same as those under § 10(b) of the Exchange Act.
- Exchange Act § 9(a)(2) makes it unlawful "[t]*o effect…a series of transactions…creating actual or apparent active trading in* [a security]*, or raising or depressing the price* [of a security]*, for the purpose of inducing the purchase or sale of such security by others.*" The SEC takes the position that cancelled or unconsummated orders can be a "*transaction*" that "*create*[es] *actual or apparent active trading*."[39]

(iv) *SEC current practice*

Since 2011, the SEC has brought 13 spoofing cases against a total of 56 defendants for alleged spoofing in relation to securities. Forty-four defendants were individuals and 12 defendants were organizations. Three defendants were found liable after trial, 27 settled their matters prior to trial, and the proceedings against the remaining 26 are pending. Notably, with the exception of one case, all of the SEC's modern spoofing cases were settled before engaging in full-scale litigation. The only case to go to trial, *SEC v. Lek Securities Corp., et al,* No. 17-CV-1789 (D.N.J.), ended in a finding of liability in November 2019.

Civil monetary penalties can be imposed on a defendant found liable in an administrative proceeding for violating Exchange Act §§ 9(a)(2) and 10(b). *See* 15 U.S.C. §§ 78u-2(a)(2) and 78u3. For each act or omission, the maximum penalty ranges from $5,000 (or $50,000 for a company) to $100,000 (or $500,000 for a company). Where the penalty falls on the spectrum is dependent on the level of intent and impact on actual or potential victims.[40] Other administrative remedies can include both temporary and permanent cease and desist orders, disgorgement, and orders barring persons from serving as an officer or director of an issuer of registered securities.[41]

Defendants can also be found civilly liable in federal district courts. The maximum penalties are the same as in administrative proceedings.[42] Both civil and administrative actions brought by the SEC must be commenced within five years from the date when the claim first accrued.[43]

In the spoofing cases brought by the SEC against organizations since 2011, monetary sanctions ranged from $250,000 to $35 million, with an average of approximately $4.46 million per organization and a median of $876,842. In the cases brought against individuals, sanctions ranged from $75,000 to $17.1 million, with an average of approximately $2.14 million per individual and a median of $417,608.

---

[35] 15 U.S.C. §§ 78i(a)(2) and 78j.
[36] 15 U.S.C. § 77q(a).
[37] *Santa Fe Indus. v. Green,* 430 U.S. 462, 476 (1977) (citation omitted).
[38] *Ernst & Ernst v. Hochfelder* 425 U.S. 185, 199 (1976).
[39] *See In re Biremis Corp.,* EA Release No. 68456, at *10-11 (Dec. 18, 2012).
[40] *See* 15 U.S.C. §78u-2(b).
[41] *See* 15 U.S.C. § 78u3.
[42] *See* 15 U.S.C. § 78u(d)(3).
[43] *See* 15 U.S.C. § 2462.

The regulation of spoofing in the US in the future

The uptick in spoofing enforcement activity in relation to derivatives, coupled with new case law that facilitates government enforcement, suggests that the DOJ and CFTC will continue to robustly pursue criminal and civil enforcement efforts going forward. Courts have rejected several legal challenges to the CEA's anti-spoofing provision, including a finding that the statutory definition of spoofing is sufficiently definite such that "*ordinary people*" can understand the scope of prohibited conduct.[44] Courts have also rejected challenges to the prosecution of spoofing under the wire fraud statute, which carries a 10-year limitation period in certain circumstances—as opposed to the five-year limitation period under the CEA's specific anti-spoofing provision—enabling prosecutors to pursue more dated conduct. That said, complicated market dynamics and trading practices will continue to present meaningful challenges for both DOJ prosecutors and civil enforcement lawyers. For example, it is commonplace for traders to place an order with the intent to execute, but then cancel it (sometimes quickly) for legitimate reasons. In the absence of "smoking gun" evidence, it is often difficult to distinguish between legitimate trading and order practices and nefarious price manipulation.

For a detailed account of relevant US enforcement actions and private civil litigation related to spoofing, as well as key judicial opinions, please refer to "*A Practice Guide on the Law of Spoofing in the Derivatives and Securities Markets*".[45]

Spoofing: the UK regime

Unlike in the US, there is no specific criminal or civil/regulatory offence of spoofing in the UK. However, the conduct that spoofing comprises typically falls within certain criminal offences under the Financial Services Act 2012 (the "**FSA 2012**") and the Fraud Act 2006, and/or within the civil regime concerning market manipulation under the EU Market Abuse Regulation (596/2014) (as imported into UK law at the end of the Brexit transition period) ("**MAR**").

While there have not been any criminal prosecutions of spoofing-related conduct in the UK to date, the FCA has taken enforcement action against individuals and firms on a number of occasions (summarised below and in the Appendix).[46] Further, the FCA "*has increased its capability to detect and take robust action against the harm to shareholder value*" caused by market manipulation,[47] and there are growing indications that it will be increasing its enforcement activity against spoofing-related activity in the future.

The UK criminal regime

(i) Legal framework

Spoofing-related activity potentially falls within the remit of the criminal offences relating to (i) the giving of false or misleading impressions under s.90 of the FSA 2012 (the "**FSA Offence**")[48], and/or (ii) the dishonest

---

[44] *United States v. Coscia*, 866 F.3d 782, 792, 93 (7th Cir. 2017).

[45] Available at https://www.milbank.com/en/news/milbank-publishes-a-practice-guide-on-the-law-of-spoofing-in-the-derivatives-and-securities-markets.html.

[46] The FCA is the UK's competent authority in respect of MAR and, separately, may bring criminal prosecutions under the FSA 2012 and the Fraud Act 2006.

[47] The FCA, "*FCA fines and prohibits hedge fund Chief Investment Officer for market abuse*", 15 December 2020 (https://www.fca.org.uk/news/press-releases/fca-fines-and-prohibits-hedge-fund-chief-investment-officer-market-abuse), per Mark Steward, Executive Director of Enforcement and Market Oversight. The comment was made in respect of the FCA's adverse finding against Corrado Abbattista, a portfolio manager who was found to have engaged in spoofing-related conduct – see further in this regard below.

[48] Certain spoofing-related activity may also be covered by s.89 FSA 2012. Under this provision, it is an offence if a person makes a statement he knows to be materially false or misleading (or is reckless in this regard or dishonestly conceals material facts), with the intention of inducing another person to take certain actions in respect of a

giving of false representations under s.2 of the Fraud Act 2006 (the "**Fraud Offence**").[49]

- Under s.90 of the FSA 2012, it is an offence if a person engages in any course of conduct which creates a false or misleading impression as to the market in, or the price or value of, any relevant investments, with the intention of creating the impression, and: (i) that person intended, by creating the impression, to induce another person to take (or refrain from taking) some action in respect of the investments; and/or (ii) the person knows that the impression is false or misleading (or is reckless in this regard) and intends to make a gain (for himself or another), or cause loss to another, by creating the impression (or is aware that creating the impression is likely to produce these results).
    - Accordingly, and although the law remains untested in relation to spoofing, for a successful prosecution, it is necessary to establish that the defendant's conduct created a false or misleading impression in the market, as well as certain elements of the defendant's intentions: i.e., that it was the defendant's intention (a) to create the impression (FSA 2012, s.90(1)), and (b), by doing so, to induce another person to take some action in relation to the investment (FSA 2012, s.90(2)), and/or to cause loss to another (or gain to the defendant (or another party)) (and knowing, or being reckless as to whether, the impression is false or misleading) (FSA 2012, s.90(3)).
    - This may be contrasted with the specific prohibition on spoofing under US law, which requires that a defendant intend, at the time of placing the relevant order, to cancel that order before execution.[50]
    - Further, it is a defence for a defendant to show (among other things) that, in relation to the offence under s.90(2) of the FSA 2012, he reasonably believed that the conduct in question would not create an impression that was false or misleading.[51]
- Under s.2 of the Fraud Act 2006, it must be shown that the defendant dishonestly made a false representation, and intended by that representation to make a gain (for himself or another person), or to cause loss to another, or to expose another person to a risk of loss.
- At present, these offences are punishable by an unlimited fine and/or imprisonment of up to seven years (in respect of the FSA Offence) and ten years (in respect of the Fraud Offence).[52]
- There is no limitation period for these criminal offences.

(ii) Current practice

Prosecutions of these offences in the context of spoofing-related conduct would likely be brought by the FCA (although the Fraud Offence might be prosecuted by another agency in certain circumstances, such

---

relevant agreement or investment. However, for the purposes of this analysis, we concentrate on the offence under s.90 FSA 2012, which appears more directly relevant to spoofing-related conduct.

[49] The potential application of these offences to spoofing-related conduct was confirmed by the High Court (albeit in the context of extradition proceedings) in *Navinder Singh Sarao v The Government of the United States of America* [2016] EWHC 2737 (Admin), [27]. *See also*: The FCA Handbook, FCG 8.1.2 (https://www.handbook.fca.org.uk/handbook/FCG/8/?view=chapter).

[50] CEA, § 4c(a)(5)(C) prohibits "*any trading, practice, or conduct on or subject to the rules of a registered entity that . . . is, is of the character of, or is commonly known to the trade as, **'spoofing' (bidding or offering with the intent to cancel the bid or offer before execution)**.*" 7 U.S.C. § 6c(a)(5)(C) (2012). (Emphasis added.)

[51] FSA 2012, s.90(9)(a).

[52] The penalties pursuant to the FSA Offence will in due course be impacted by the Financial Services Act 2021, which will increase the maximum sentence for these offences to 10 years once s.31 enters into force. At the time of writing, however, s.31 does not yet have a confirmed commencement date.

as the Serious Fraud Office where a serious or complex fraud is the predominant issue).[53]

However, as noted above, no prosecutions have been brought to date (in contrast to the position under the civil/regulatory regime, as described below). This may be due to various factors where spoofing-related conduct is concerned, including the difficulty of establishing intent (including that an order was cancelled due to a spoofing-related strategy (rather than for other reasons)), and the higher standard of proof in UK criminal proceedings (i.e., beyond reasonable doubt).

The UK civil/regulatory regime

(i) Legal framework

The civil prohibition under MAR that a person "*shall not engage in or attempt to engage in market manipulation*"[54] is extended (by Articles 12(1) and (2)) to a range of investment and trading activities, including acts that would likely be regarded as being, or relating to, spoofing. The following activities, for example, are expressly deemed to be forms of market manipulation (emphasis added):

- "*entering into a transaction,* ***placing an order to trade*** *or any other behaviour which (i)* ***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 (ii) 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…*" (save where there are "*legitimate reasons*" and the practice conforms to accepted market practice under Article 13) (MAR, Article 12(1)(a)); and
- "*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***" (MAR, Article 12(1)(b)).
- In addition, MAR, Article 12(2)(c) applies to the placing (and/or cancellation or modification) of orders on a trading system that has any of the effects referred to above by, for example, "*(ii) 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…*" or "*(iii) creating or being likely to create a false or misleading signal about the supply of, or demand for, or price of, a financial instrument…*".
- Moreover, MAR, Recital 46 confirms that "[m]*anipulation or attempted manipulation of financial instruments may also consist in placing orders which may not be executed*".

Annex 1 to MAR[55] lists various indicators of manipulative behaviour relating to (respectively) "*false or misleading signals and to price securing*" and "*the employment of a fictitious device or any other form of deception or contrivance*". A number of these indicators relate to the effects of orders to trade given (or cancelled). However, the FCA has previously commented that, in the context of market abuse risk assessments, "*the lists in MAR are not exhaustive*", noting that firms that treat them as such may fail to

---

[53] FCA Handbook, EG App 2.1.9(b). As noted in EG 12.4.1, the FCA agreed guidelines (at Enforcement Guide, Appendix 2) with a number of agencies (such as the Crown Prosecution Service or Serious Fraud Office) that establish a framework that, among other things, assists the agencies in determining which one may pursue an enforcement action where more than one may have an interest in doing so.

[54] MAR, Article 15.

[55] Delegated Regulation (EU) 2016/522, Annex II (as imported into UK law following the end of the Brexit transition period) supplements this list.

detect and report "*other types of market manipulation which are still within the broader scope of MAR article 12(1)(a) and (b)*".[56]

Under MAR's approach to regulating market manipulation, it is not necessary to prove that a trader specifically intended to engage in market abuse. In this regard, the FCA has confirmed 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.*"[57] However, the High Court confirmed in *Burford Capital Limited v London Stock Exchange Group plc*[58] that, "[d]*epending on what that* [false or misleading] *signal is (an objective question, to be sure), falsity might involve some subjective enquiry*" in that the truth or falsity of the relevant signals may turn on the actual intentions of the trader in question.[59]

If a breach of MAR is established, the FCA may seek injunctive relief, prohibit regulated firms or individuals from performing regulated activities, and/or impose an unlimited fine.[60]

In relation to any offence under MAR, there is no applicable limitation period. If the FCA were to bring enforcement action against an individual for a breach of the Statements of Principle (e.g., proper standards of market conduct) or for being knowingly concerned in the breach by a firm of the Principles for Businesses, this would be subject to a six-year limitation period, which begins to run from the first day on which the FCA (a) knows of the misconduct, or (b) has information from which the misconduct can reasonably be inferred.[61]

(ii) Current practice

The FCA has expressed concerns about spoofing-related activity for a number of years.[62] While the FCA has previously taken enforcement action relating to spoofing (as summarised below and in the Appendix) and has also played a role in assisting cross-border enforcement activity,[63] there are signs that spoofing-related conduct is an area in which the FCA is becoming increasingly active.

---

[56] The FCA, "*Market Watch, Issue 56*", September 2018 (https://www.fca.org.uk/publication/newsletters/market-watch-56.pdf), p.2.

[57] Speech by Julia Hoggett, formerly Director of Market Oversight, the FCA, "*Effective compliance with the Market Abuse Regulation – a state of mind*", 14 November 2017 (https://www.fca.org.uk/news/speeches/effective-compliance-market-abuse-regulation-a-state-of-mind). *See also*: The FCA Handbook, MAR 1.2.3G ("*The Market Abuse Regulation does not require the person engaging in the behaviour in question to have intended to commit market abuse*").

[58] [2020] EWHC 1183 (Comm).

[59] *Id.*, [50] to [53]. For a practical example of this, *see* the FCA final notice dated 15 December 2020 in relation to Mr Abbattista (https://www.fca.org.uk/publication/final-notices/corrado-abbattista-dec-2020.pdf), which notes (at p.20) that "*Mr Abbattista* ***must have been aware of the risk that his actions might constitute market abuse, in that his Misleading Orders would give false or misleading signals*** *to other market participants as to the supply of, or demand for, shares in the Companies, but recklessly went ahead with them anyway*." (Emphasis added.)

[60] *See* https://www.fca.org.uk/markets/market-abuse.

[61] Financial Services and Markets Act 2000 ("**FSMA 2000**"), ss.60(1), 60(4), 60(5) and 60(5ZA) (the latter provision as introduced by the Financial Services (Banking Reform) Act 2013, s.28(6)).

[62] *See*, for example, the concern the FCA expressed in relation to "layering and spoofing" in August 2009 in Issue 33 of its *Market Watch* newsletter (https://webarchive.nationalarchives.gov.uk/20130412191747/http://www.fsa.gov.uk/pubs/newsletters/mw_newsletter33.pdf).

[63] *See*, for example, *In re Mirae Asset Daewoo Co., Ltd., CFTC Dkt. No. 20-11* (Jan. 13, 2020), in which the FCA (among others) co-operated in a US enforcement action (against spoofing-related conduct) being prosecuted by the CFTC.

In March 2020, the FCA indicated that it had five active investigations concerning spoofing-related conduct,[64] and in April 2020 it announced (as one of its key outcomes for 2020/2021) "[c]*lean markets that make it difficult to commit market abuse and financial crime*".[65] Later in 2020, the FCA imposed a prohibition on the performance of any regulated activities and a £100,000 fine on Corrado Abbattista, a portfolio manager at Fenician Capital Management LLP in London,[66] for engaging in market manipulation (as defined in MAR, Article 12(1)(a)). The FCA found that Mr Abbattista, for several months in 2017, "*placed large orders (by reference to the average order size in those shares in the market at that time) for* [certain equity contracts for differences] *which he did not intend to execute … on the opposite side of the order book to existing smaller orders which he intended to execute*".[67] The FCA determined that Mr Abbattista "*gave false and misleading signals as to demand/supply*" because he did not place these large orders with a genuine intention that they should be executed, and they were for volumes of shares "*far greater than the typical market size*", meaning that they would likely have had a material impact on other market participants.[68]

This increase in the FCA's focus on spoofing-related activity may be the result of a number of factors. These include:

- the FCA's active monitoring of transaction data, provided by UK trading venues, firms and individuals who professionally arrange or execute transactions, as a result of suspicious transaction and order reports;[69]
- the operation of the FCA's internal surveillance systems by which it "*ingests order book data from the leading UK equity trading venues and then runs surveillance algorithms, designed to identify potentially abusive behaviours, across that consolidated data set*"[70] – for example, in respect of secondary market surveillance, the FCA in 2019 "*ingested close to 10 billion transaction reports and over 150 million order reports every day into* [its] *market data processor*";[71] and

---

[64] FCA response to freedom of information request dated 18 March 2020: https://www.fca.org.uk/publication/foi/foi7123-response.pdf. By way of comparison, the FCA did not open any spoofing-related investigations in 2019, and only opened one in 2018.

[65] The FCA, Business Plan 2020/21, 7 April 2020 (https://www.fca.org.uk/publications/corporate-documents/our-business-plan-2020-21), p.21.

[66] The FCA, "*FCA fines and prohibits hedge fund Chief Investment Officer for market abuse*", 15 December 2020 (https://www.fca.org.uk/news/press-releases/fca-fines-and-prohibits-hedge-fund-chief-investment-officer-market-abuse). While Mr Abbattista initially referred this decision to the Upper Tribunal, he withdrew that reference on 10 November 2020.

[67] The FCA final notice dated 15 December 2020 in relation to Mr Abbattista (https://www.fca.org.uk/publication/final-notices/corrado-abbattista-dec-2020.pdf), p.2.

[68] *Id.* The FCA also noted that the false, large orders were placed such that their full size was visible to other market participants, but the genuine orders were placed as "iceberg orders" (whereby only a portion of the orders would be visible to other market participants).

[69] *See*, for example: The FCA, "*Annual Report and Accounts 2019/20*", 10 September 2020 (https://www.fca.org.uk/publication/annual-reports/annual-report-2019-20.pdf), p.37.

[70] The FCA, "*FCA fines and prohibits hedge fund Chief Investment Officer for market abuse*", 15 December 2020 (https://www.fca.org.uk/news/press-releases/fca-fines-and-prohibits-hedge-fund-chief-investment-officer-market-abuse). Notably, this mechanism was used in the enforcement action against Mr Abbattista.

[71] Speech by Mark Steward, Executive Director of Enforcement and Market Oversight, the FCA, "*Capital market regulation and coronavirus*", 7 August 2020 (https://www.fca.org.uk/news/speeches/capital-market-regulation-and-coronavirus).

- the operation of the FCA's power to issue information requests to trading venues and firms for their order book data in order to support its enquiries.[72]

However, it is important to note that the extensive data analysis deployed by the FCA does not necessarily lead to more findings of market manipulation: in *Burford Capital Limited v London Stock Exchange Group plc*, the FCA concluded that, on the basis of the full range of evidence which was available to it, there was no reason to think that unlawful market manipulation had taken place.[73] Similarly, trading data analysis triggered an FCA review into spoofing-related conduct by Mr King Yew Choo (formerly a junior trader at Citigroup Global Markets Limited). Although the FCA provisionally considered Mr Choo "*to have received an improved execution price as a result of buying or selling relatively soon after manually adjusting Citigroup's quotes* [in certain Slovenian government bonds] *to achieve a new Best Offer or Bid*" on the relevant trading platform without legitimate explanation, the FCA ultimately decided that it was not "*appropriate to take any further action in relation to this particular event*."[74]

The regulation of spoofing in the UK in the future

The FCA's increased activity during 2020-21 indicates that the FCA is targeting market manipulation[75] and, within that, spoofing-related activity, with increasing rigour.[76] Further, through its growing data ingestion and analysis capabilities, the FCA may be increasingly well-positioned to overcome evidential hurdles relating to spoofing-related conduct.

In light of this developing enforcement strategy, firms that are regulated by the FCA should ensure that their internal systems and controls are sufficiently sophisticated to monitor and mitigate any risks relating to spoofing-related activity (as well as market manipulation in general).

---

[72] *See*: The FCA, "*Market Watch, Issue 67*", 28 May 2021 (accessible at: https://www.fca.org.uk/publications/newsletters/market-watch-67).

[73] *See* our previous Client Alert: Milbank LLP, "*Burford Capital v London Stock Exchange Group PLC: disclosure in support of market manipulation claims*", 28 May 2020 (https://www.milbank.com/en/news/burford-capital-v-london-stock-exchange-group-plc-disclosure-in-support-of-market-manipulation-claims.html).

[74] *Mr K Y Choo v Citigroup Global Markets Ltd*: 3201735/2019, Judgment with Reasons, [25] to [35]. The FCA did, however, note that it expected Citigroup to discuss the contents of the letter with Mr Choo and other relevant parties at the firm, including the head of the relevant business area and Internal Audit.

[75] Recently, for example, the FCA imposed a financial penalty of £52,500 and a prohibition on performing any functions in relation to a regulated activity on a senior market-making trader after it found that he had carried out 129 "wash trades" (in essence, trades executed with himself) between July 2018 and May 2019 in order artificially to increase the share trading volume of a company such that it would remain in the FTSE All Share Index: *see* the FCA's final notice dated 3 March 2021 in relation to Mr Horn (available at: https://www.fca.org.uk/publication/final-notices/adrian-horn.pdf).

[76] It should be noted that the FCA is not the only UK regulator with an apparently increasing appetite in this regard: In April 2020, Ofgem imposed a £35m fine (subsequently reduced by way of settlement discount) against InterGen "*after an investigation found that InterGen sent misleading signals to National Grid Electricity System Operator*": *see* https://www.ofgem.gov.uk/publications-and-updates/ofgem-requires-intergen-pay-37m-over-energy-market-abuse. Market manipulation (which includes spoofing-related activity) is prohibited in the wholesale energy markets by the EU Regulation on Wholesale Energy Market Integrity and Transparency (1227/2011), as incorporated into UK law following the end of the Brexit transition period.

APPENDIX

SUMMARIES OF COMPLETED FCA ENFORCMENT ACTIONS CONDUCTED IN RESPECT OF SPOOFING-RELATED CONDUCT TO DATE

FCA final notice issued to Michael Coscia dated 3 July 2013[77]

- Mr Coscia was an experienced market participant with 25 years' trading experience who traded from the US through a Direct Market Access provider.[78] In July 2013, the FCA fined him $903,176[79] after it found him to have deliberately engaged in the "layering" of commodities futures on the ICE Futures Europe exchange (on his own proprietary account) during six weeks of trading in late 2011. Mr Coscia had developed an automated algorithmic programme that effected trades at a faster rate than would be feasible via manual order entry.[80]

- The FCA found that Mr Coscia had "*placed and rapidly cancelled large orders which he did not intend to trade with the intention of creating a false impression as to the weight of buyer or seller interest thereby "layering" the order book and manipulating the market*."[81] It was held that this conduct amounted to "*deliberate market abuse (market manipulation)*" in breach of FSMA 2000, s.118(5).[82]

7722656 Canada Inc (formerly carrying on business as Swift Trade Inc) and another v FCA [2013] EWCA Civ 1662

- In these proceedings, the FCA (then the Financial Services Authority) had sought to impose an £8 million fine on Swift Trade for engaging in systematic "layering"[83] in respect of certain orders of contracts for differences placed in relation to shares traded on the London Stock Exchange ("**LSE**"). Once these orders were placed, they had then been hedged by automated orders to buy or sell an equivalent quantity of the shares ordered. Within a short time of the original orders being placed, they were cancelled and the consequent hedging orders were also (automatically) cancelled, "*but*

---

[77] Available at https://www.fca.org.uk/publication/final-notices/coscia.pdf.

[78] *Id.*, p.2. "Direct Market Access" is a service offered by some stockbrokers who are exchange member firms that enables investors to place buy and sell orders directly on the orderbook.

[79] This amount includes a 30% discount applied by the FCA for Mr Coscia's early settlement of the matter.

[80] The FCA final notice dated 3 July 2013 in relation to Mr Coscia (https://www.fca.org.uk/publication/final-notices/coscia.pdf), pp.2-3.

[81] *Id.*, p.1.

[82] Prior to MAR, the FCA (formerly the Financial Services Authority) prosecuted civil spoofing-related enforcements under FSMA 2000, s.118(5). This provision was repealed with effect from the date that MAR took effect.

[83] The Court of Appeal considered the following definition of "layering" useful (per [2013] EWCA Civ 1662, [4]): *""layering" consists of the practice of entering relatively large orders on one side of an exchange's (in this case the* [London Stock Exchange's]*) electronic order book ("the order book") without a genuine intention that the orders will be executed: the orders are placed at prices which are (so the person placing them believes) unlikely to attract counterparties, while they nevertheless achieve his objective of moving the price of the relevant share as the market adjusts to the fact that there has been an apparent shift in the balance of supply and demand. The movement is then followed by the execution of a trade on the opposite side of the order book which takes advantage of, and profits from, that movement. This trade is in turn followed by a rapid deletion of the large orders which had been entered for the purpose of causing the movement in price, and by repetition of the behaviour in reverse on the other side of the order book. In other words, a person engaged in layering attempts to move the price up in order to benefit from a sale at a high price, then attempts to move it down in order to buy again, but at a lower price, and typically repeats the process several times*."

there would meanwhile have been a movement of the shares utilised in the hedge of which [Swift Trade] *could take advantage*."[84]

- The Upper Tribunal had concluded that Swift Trade's trading was a breach of FSMA 2000, s.118(5), noting that it was "*deliberate, manipulative, designed to deceive other marker users, successful in that aim and undertaken for motives of profit*".[85] The Court of Appeal dismissed Swift Trade's appeal against this decision,[86] leading the FCA to impose an £8 million fine against Swift Trade.

***FCA v Da Vinci Invest Ltd and others* [2015] EWHC 2401 (Ch)**

- In these proceedings, the FCA sought a final injunction and to affirm a penalty of £7.57 million against certain traders and Da Vinci Invest Ltd in respect of market manipulation (in the form of spoofing) that it had found had taken place in 2010 and 2011. The activity had occurred in the course of high-volume trading in contracts for differences in relation to shares traded on the LSE.[87]

- The High Court was "*entirely satisfied*" that the defendants had engaged in market manipulation within FSMA 2000, s.118(5).[88] The Court accepted that there was a repeated pattern whereby: the traders (via automated algorithms) placed a series of orders on the LSE and then immediately placed corresponding orders to move the prices of the shares, after which the traders would aggressively enter orders on the other side of the order book from their net order position; the traders would then trade with large orders recently entered by market participants at prices at or close to the best bid or offer price; once these trades had executed, the traders would reverse their position on the order book by cancelling their existing orders. The Court found that the result of this was that the traders "*were able to buy shares at lower prices when the market fell, and sell them at higher prices when the market rose*."[89] Further, the repeated patterns of trading were "*too similar and too frequent to be the result of coincidence or some other innocent strategy*."[90] This conduct gave a false or misleading impression to other market participants of an increased supply or demand for the shares in question, since the traders in fact 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*."[91] The FCA's penalty was therefore affirmed.

FCA final notice issued to Paul Walter dated 22 November 2017[92]

- Mr Walter was an experienced trader in government bonds who was employed by Bank of America Merrill Lynch International Limited during the relevant period. In November 2017, the FCA fined him £60,090 for, in twelve instances during 2014, "*entering quotes … in relation to six Dutch State Loans… that were designed to induce, and had the effect of inducing, other market participants*

---

[84] [2013] EWCA Civ 1662, [6].
[85] *Id.*, [3] and [9].
[86] *See id.*, [11] to [36]. Swift Trade had contended that the relevant entity had not existed at the time that the FCA's decision notice was issued, and that contracts for differences were not "qualifying investments" for the purpose of FSMA 2000, s.118(5).
[87] [2015] EWHC 2401 (Ch), [1].
[88] *Id.*, [164].
[89] *Id.*, [149] to [154].
[90] *Id.*, [154].
[91] *Id.*, [163]. The Court also emphasised that "*the reference in section 118(5) to behaviour that is "likely to give a false or misleading impression" focuses attention on the likely perception of other parties, not the state of mind of the person whose behaviour is under consideration*" (at [107]). The Court went on to apply *dicta* in *Winterflood Securities Limited v FSA* [2010] EWCA Civ 423 (at [25]) 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*" ([108]).
[92] Accessible at https://www.fca.org.uk/publication/final-notices/paul-axel-walter-2017.pdf.

who were tracking quotes to raise or lower their quotes". Mr Walter benefitted by subsequently cancelling his own quote and buying or selling at a better price at the artificial level achieved by effecting this "*false and misleading impression as to the price and supply or demand*" of the Dutch State Loans in breach of FSMA 2000, s.118(5).[93]

- In taking these steps, the FCA noted that Mr Walter knew that certain market participants used automated systems that he could take advantage of "*to attract these algorithms to follow his quotes and so sell or buy the* [Dutch State Loans] *at higher or lower prices*."[94] However, the FCA found that the abuse had been committed negligently rather than deliberately as "*he did not appreciate (although he was negligent in not doing so) that his actions constituted market abuse and therefore would not have realised that he was risking his career and reputation by acting as he did*."[95] Nonetheless, the FCA considered it to be a serious example of market abuse because: he was an experienced trader of government bonds; he should have realised that his behaviour constituted market abuse (particularly after he was put on notice of concerns about his behaviour); and his behaviour by its nature undermines confidence in the UK markets.[96]

FCA final notice issued to Corrado Abbattista dated 15 December 2020

Please see the section "The UK civil/regulatory regime" in the body of the briefing above for a summary of this FCA enforcement action.

---

[93] *Id.*, pp.1-3.
[94] *Id.*, p.2.
[95] *Id.*, p.33. It was also relevant that the financial profit from the relevant trades was insignificant to the bank.
[96] *Id.*, p.3.

Global Litigation Contacts

London | 10 Gresham Street, London EC2V 7JD

Name	Email	Phone
Tom Canning	tcanning@milbank.com	+44 20.7615.3047
William Charles	wcharles@milbank.com	+44 20.7615.3076
Charles Evans	cevans@milbank.com	+44 20.7615.3090
Julian Stait	jstait@milbank.com	+44 20.7615.3005
Mona Vaswani	mvaswani@milbank.com	+44 20.7615.3002

New York | 55 Hudson Yards, New York, NY 10001-2163

Name	Email	Phone
George S. Canellos, *Global Head of Litigation*	gcanellos@milbank.com	+1 212.530.5792
Daniel Perry, *Practice Group Leader*	dperry@milbank.com	+1 212.530.5083
Wayne M. Aaron	waaron@milbank.com	+1 212.530.5284
Antonia M. Apps	aapps@milbank.com	+1 212.530.5357
Thomas A. Arena	tarena@milbank.com	+1 212.530.5828
James G. Cavoli	jcavoli@milbank.com	+1 212.530.5172
Scott A. Edelman, *Firm Chairman*	sedelman@milbank.com	+1 212.530.5149
Adam Fee	afee@milbank.com	+1 212.530.5101
Christopher J. Gaspar	cgaspar@milbank.com	+1 212.530.5019
David R. Gelfand	dgelfand@milbank.com	+1 212.530.5520
Robert C. Hora	rhora@milbank.com	+1 212.530.5170
Alexander Lees	alees@milbank.com	+1 212.530.5161
Grant Mainland	gmainland@milbank.com	+1 212.530.5251
Atara Miller	amiller@milbank.com	+1 212.530.5421
Sean M. Murphy	smurphy@milbank.com	+1 212.530.5688
Tawfiq S. Rangwala	trangwala@milbank.com	+1 212.530.5587
Stacey J. Rappaport	srappaport@milbank.com	+1 212.530.5347
Fiona A. Schaeffer	fschaeffer@milbank.com	+1 212.530.5651
Jed M. Schwartz	jschwartz@milbank.com	+1 212.530.5283
Alan J. Stone	astone@milbank.com	+1 212.530.5285

Washington, DC | International Square Building, 1850 K Street, NW, Suite 1100, Washington, DC 20006

Name	Email	Phone
David S. Cohen	dcohen2@milbank.com	+1 202.835.7517
Andrew M. Leblanc	aleblanc@milbank.com	+1 202.835.7574
Michael D. Nolan	mnolan@milbank.com	+1 202.835.7524
Aaron L. Renenger	arenenger@milbank.com	+1 202.835.7505

Los Angeles | 2029 Century Park East, 33rd Floor Los Angeles, CA 90067-3019

Name	Email	Phone
Lauren N. Drake	ldrake@milbank.com	+1 424.386.4320
Gary N. Frischling	gfrischling@milbank.com	+1 424.386.4316
David I. Gindler	dgindler@milbank.com	+1 424.386.4313
Robert J. Liubicic	rliubicic@milbank.com	+1 424.386.4525
Y. John Lu	jlu@milbank.com	+1 424.386.4318
Alex G. Romain	aromain@milbank.com	+1 424.386.4374

Munich | Maximilianstraße 15, 80539 Munich

Ulrike Friese-Dormann	ufriese@milbank.com	+49 89.25559.3646
Peter Nussbaum	pnussbaum@milbank.com	+49 89.25559.3636
Alexander Rinne	arinne@milbank.com	+49 89.25559.3686
Christoph Rothenfusser	crothenfusser@milbank.com	+49 89.25559.3656

Litigation & Arbitration Group

Please feel free to discuss any aspects of this Dispute Resolution Briefing with your regular Milbank contacts or any of the members of our global Litigation & Arbitration Group.

This Dispute Resolution Briefing is a source of general information for clients and friends of Milbank LLP. Its content should not be construed as legal advice, and readers should not act upon the information in this Dispute Resolution Briefing without consulting counsel.

© 2021 Milbank LLP

All rights reserved.