GT GreenbergTraurig

Alert | White Collar Defense & Special Investigations

January 2021

Financial Fraud Enforcement Priorities for 2021 and Beyond (White Collar Insights - 2021 Outlook Series - Part 2)

In recent years, the federal government's financial fraud enforcement priorities have been largely consistent and robust. But in 2020, the pandemic appeared to cause government authorities to focus more resources to combat financial fraud as it related to COVID-19. In 2021, we may see an uptick in enforcement actions because of new priorities set by a Biden administration and because of fraudulent activities associated with the pandemic. As discussed below, there are multiple areas of financial fraud enforcement to watch.

Insider Trading

Over the last decade, insider trading has been a key enforcement priority for the U.S. Department of Justice (DOJ) and the Securities and Exchange Commission (SEC) and will likely continue to be one for quite some time. While the DOJ and SEC have been leading the charge in this enforcement area, with the advent of authorities granted under the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010, the Commodity Futures Trading Commission (CFTC) has also become a significant player in the government's pursuit of insider trading enforcement. DOJ prosecutors — particularly those from the U.S. Attorney's Office for Southern District of New York (SDNY) — and SEC/CFTC enforcement attorneys have brought several headline-grabbing cases in this area, and given some of the trading activity witnessed during COVID-19, including those by some members of Congress immediately before the pandemic took

© 2021 Greenberg Traurig, LLP

hold back in February 2020, we could see an uptick in the number of charged cases in the coming year. To this end, in March 2020, the SEC's former co-directors of enforcement made clear in a rare public statement that the SEC is watching for potential insider trading during this time of national crisis.

Insider trading is a unique area of enforcement, as there is no statute that defines its elements. Instead, the prohibition against insider trading is premised on caselaw interpretation of the anti-fraud provisions of section 10(b) of the Securities and Exchange Act of 1934. Essentially, insider trading law is based on proscribing the use, trading, and/or tipping of material non-public information (MNPI) in breach of a duty, whether that be a duty to a company's shareholders (the "classical theory") or a duty to a source that imparted the MNPI under a confidentiality agreement or pursuant to a fiduciary duty (the "misappropriation theory"). But there have been several areas of contentious litigation, including cases that have reached the Supreme Court, over the elements that constitute the offense. For example, for the conduct to be unlawful, one who tips MNPI in breach of a duty must receive a "personal benefit"; substantial litigation has generated, particularly in the Second Circuit, over what constitutes such a benefit.

Given some of the competing views defining the offense, the government has largely adhered to charging cases based on favorable caselaw interpretation. Further, the government has recently used some (relatively) new arrows in its quiver in making charging decisions, including by charging insider trading using a securities fraud statute enacted under the Sarbanes-Oxley Act, which the government has argued (and some courts have agreed) does not require proof of the same elements of insider trading as under section 10(b) of the Exchange Act. Moreover, the government is particularly focused on insider trading involving so-called "political intelligence" — trading based on potentially market-moving information emanating from the federal government (e.g., impending announcements about Medicare/Medicaid reimbursement rates). When the dust settles from the pandemic, the DOJ and SEC may charge more insider trading cases based on information regarding COVID-19 and/or material decisions made by companies in response to the pandemic, including cases that involve political intelligence. In short, the unrelenting pace of insider trading enforcement may well continue unabated.

Mismarking/Valuation Fraud

Following the 2008 financial crisis, the government brought several notable mismarking/valuation fraud enforcement actions, particularly with respect to those involving illiquid securities. During periods of economic turmoil, underlying fraudulent financial schemes may be discovered when those schemes can no longer suppress the illusion of enhanced value. Before that point, it can be particularly challenging to value illiquid assets due to impeded visibility into underlying valuation mechanisms and the relative ease by which the independent valuation process can be corrupted. Consequently, illiquid assets may be especially susceptible to fraud.

We may see an uptick in the number of mismarking/valuation fraud actions brought by the DOJ and SEC in the coming years. The economic devastation and market volatility caused by COVID-19 may reveal schemes involving the mismarking of illiquid securities as certain financial products are devalued and investors withdraw and redeem from funds. At this juncture, firms may wish to review their valuation procedures, spot-check illiquid valuations, and establish robust training to avoid concerns over their valuation policies.

Accounting Fraud

We may see an increased emphasis by the DOJ and SEC in policing accounting fraud. In times of crisis and market volatility, there is a concern that publicly traded companies and executives could be inclined

© 2021 Greenberg Traurig, LLP

to manipulate earnings or engage in other forms of accounting fraud. Before and after the Great Recession, there were several DOJ and SEC actions concerning manipulated earnings, falsified financials, and stock-option backdating. The stresses resulting from COVID-19 may result in similar activity, and the government may similarly respond with vigorous enforcement.

One prominent DOJ office, SDNY, signaled this year that accounting fraud will be an increased priority for its white-collar criminal prosecutors. Indeed, SDNY has been pursuing a number of accounting fraud cases against senior executives of public companies relating to alleged manipulation of both GAAP and non-GAAP metrics, and that office has indicated that it intends to continue its focus on non-GAAP metric manipulation. Prosecutors also have indicated that they are interested in pre-IPO fraud, and have warned that private companies are not immune from accounting fraud. Accordingly, we may see continued criminal and civil enforcement based upon accounting fraud allegations against both public and private companies.

Cryptocurrency Enforcement

The development of cryptocurrency has been instrumental in the pursuit of more secure financial transactions. Many of cryptocurrency's central features — including decentralized operation and control and anonymity — provide a myriad of potential benefits for commercial activity beyond mere currency exchange but also present unique challenges for public safety. The DOJ, SEC, CFTC, Department of Treasury, including the Financial Crimes Enforcement Network (FinCEN), Office of Foreign Assets Control (OFAC), and the Internal Revenue Service (IRS), and even state attorneys general are focusing heavily on this new area of technology. Many agencies have been taking aggressive enforcement actions while critics have decried regulation by enforcement.

Each of the relevant government agencies has its own unique role in this space. For example, the SEC has brought actions against initial coin offerings where it views those tokens as "securities" and brought actions to stop fraudulent activities involving these tokens; the CFTC has been using its anti-fraud authorities to police the use of cryptocurrency, which it views as a commodity and thus within its purview; and the DOJ has charged individuals and entities with criminal offenses using cryptocurrency to effectuate, or as the object of, a perpetrator's scheme. There has been a significant uptick in enforcement activity involving cryptocurrency in the past year, and this increased level of activity will likely continue. For example, the SEC has recently brought multiple significant actions to enjoin coin offerings and has secured victories with judicial opinions that undermine the ability of companies to launch tokens using registration exemptions under the securities laws. The DOJ also has instituted several high-profile prosecutions involving cryptocurrency used by child exploitation rings, for terrorist financing, and as part of cyber-hacking and ransomware attacks, sanctions violations, securities fraud, and narcotics trafficking. Further, in October 2020, the Attorney General's Cyber Digital Task Force issued its first Cryptocurrency Enforcement Framework. The DOJ Task Force found that illicit activities involving cryptocurrency typically include: (1) financial transactions associated with the commission of crimes; (2) money laundering and the shielding of illegitimate activity from tax, reporting, or other legal requirements; and (3) other crimes, such as theft, directly implicating the cryptocurrency marketplace itself. Notably, the DOJ's Framework recognizes the important commercial value provided by digital assets but pledges vigilance in its enforcement activity.

Government authorities are moving in earnest to police, protect, and regulate the cryptocurrency space. We anticipate an increasingly enhanced focus on this area of enforcement in the coming years with additional high-profile governmental actions.

© 2021 Greenberg Traurig, LLP

Spoofing

Spoofing generally occurs when a trader places an order in a futures market with the intention to cancel the order prior to execution. Government agencies, including the DOJ, CFTC, and SEC, have been cracking down on spoofing in recent years. This will likely continue with criminal and civil investigations and enforcement actions in the area. Typically, traders spoof to misrepresent supply or demand in order to induce other traders to act in a way beneficial to the spoofing trader. Additional manipulative practices may be employed in spoofing, including layering trades and coordinated trading to avoid detection. Spoofing may be done manually or by using electronic trading algorithms, and the government has been pursuing both types of cases.

Recently, the government has focused on spoofing in the precious metals market, other commodities futures, and securities markets. These areas are likely to remain a focus, and there may be expanded investigations into Over the Counter (OTC), treasury futures, and other markets. The government has alerted market participants that it intends to utilize its enhanced data analytics capabilities to discover and prosecute illegal spoofing and manipulative trading. While the DOJ's record of success prosecuting such cases has been mixed, and it has lost some high-profile criminal spoofing trials, we expect criminal enforcement to continue undeterred. Further, civil investigations by the SEC and CFTC could increase in 2021, as will coordinated parallel proceedings between the civil and criminal authorities. The government has also focused on international trading, specifically trading occurring in Japan, South Korea, and India. That focus will likely continue in 2021.

The government continues to settle the majority of spoofing cases, giving substantial consideration to cooperation and self-reporting by spoofing defendants. Given the government's focus, firms may wish to maintain/develop effective compliance programs to address spoofing and other manipulative trading practices.

Cybersecurity

Cybersecurity concerns can directly and indirectly impact the stability of global banks, broker dealers, asset managers, investment funds, public companies, law firms, and others. The DOJ, SEC, and state regulators are keenly focused on cybersecurity as a critical enforcement priority. Concerns about systems vulnerability and the ability of institutions to protect confidential proprietary and customer information have only been magnified during the remote work environment of COVID-19. Even when the pandemic is over, cybersecurity and data privacy concerns will likely be a key focus of federal and state authorities for many years to come.

Government agencies have targeted cybersecurity issues from both a criminal and civil perspective. From a criminal perspective, the DOJ is particularly focused on: hacking issues and ransomware attacks; theft of trade secrets; economic espionage, particularly by China, North Korea, Iran, and Russia; identity theft; securities fraud using computer intrusion; and other financial fraud. Notably, ransomware attacks present thorny legal issues, as potential sanctions evasion and money transmission issues under the Bank Secrecy Act have been highlighted by federal authorities when victims make ransom payments. The SEC has focused on disclosure rules concerning cybersecurity efforts and breaches. And certain state regulators, such as the New York State Department of Financial Services, have issued cybersecurity regulations or guidance regarding risk assessments, securing of personally identifiable information (PII), incident response plans, and breach notification requirements. The above-referenced issues and governmental scrutiny may well be magnified with remote work in the near-term.

© 2021 Greenberg Traurig, LLP

Conclusion

In 2021, we expect government authorities to be focused on the key fraud enforcement areas discussed above. Because of fraudulent activities associated with the pandemic, and potential new priorities under a Biden administration, an overall uptick in enforcement activity, including in the areas above, seems likely. Financial institutions, companies, and individuals would be well-served to assess their compliance programs and address concerns at this juncture, before issues arise that may draw government scrutiny.

Authors

This GT Alert was prepared by:

- Daniel P. Filor | +1 212.801.6758 | filord@gtlaw.com
- David I. Miller | +1 212.801.9205 | David.Miller@gtlaw.com
- Nathan J. Muyskens | +1 202.331.3164 | muyskensn@gtlaw.com

Albany. Amsterdam. Atlanta. Austin. Boston. Chicago. Dallas. Delaware. Denver. Fort Lauderdale. Germany.¬ Houston. Las Vegas. London.* Los Angeles. Mexico City.+ Miami. Milan.» Minneapolis. New Jersey. New York. Northern Virginia. Orange County. Orlando. Philadelphia. Phoenix. Sacramento. Salt Lake City. San Francisco. Seoul.∞ Shanghai. Silicon Valley. Tallahassee. Tampa. Tel Aviv.^ Tokyo.¤ Warsaw.~ Washington, D.C.. West Palm Beach. Westchester County.

*This Greenberg Traurig Alert is issued for informational purposes only and is not intended to be construed or used as general legal advice nor as a solicitation of any type. Please contact the author(s) or your Greenberg Traurig contact if you have questions regarding the currency of this information. The hiring of a lawyer is an important decision. Before you decide, ask for written information about the lawyer's legal qualifications and experience. Greenberg Traurig is a service mark and trade name of Greenberg Traurig, LLP and Greenberg Traurig, P.A. ¬Greenberg Traurig's Berlin office is operated by Greenberg Traurig Germany, an affiliate of Greenberg Traurig, P.A. and Greenberg Traurig, LLP. *Operates as a separate UK registered legal entity. +Greenberg Traurig's Mexico City office is operated by Greenberg Traurig, S.C., an affiliate of Greenberg Traurig, P.A. and Greenberg Traurig, LLP. »Greenberg Traurig's Milan office is operated by Greenberg Traurig Santa Maria, an affiliate of Greenberg Traurig, P.A. and Greenberg Traurig, LLP. ∞Operates as Greenberg Traurig LLP Foreign Legal Consultant Office. ^Greenberg Traurig's Tel Aviv office is a branch of Greenberg Traurig, P.A., Florida, USA. ¤Greenberg Traurig's Tokyo Office is operated by GT Tokyo Horitsu Jimusho and Greenberg Traurig Gaikokuhojimubengoshi Jimusho, affiliates of Greenberg Traurig, P.A. and Greenberg Traurig, LLP. ~Greenberg Traurig's Warsaw office is operated by Greenberg Traurig Grzesiak sp.k., an affiliate of Greenberg Traurig, P.A. and Greenberg Traurig, LLP. Certain partners in Greenberg Traurig Grzesiak sp.k. are also shareholders in Greenberg Traurig, P.A. Images in this advertisement do not depict Greenberg Traurig attorneys, clients, staff or facilities. No aspect of this advertisement has been approved by the Supreme Court of New Jersey. ©2021 Greenberg Traurig, LLP. All rights reserved.*