



Regulatory Investigations and Enforcement Trends in 2022

Feb 25, 2022

Reading Time : **4 min**

By: Peter I. Altman, Karen Elizabeth Christian, Charles F. Connolly, Katherine R. Goldstein, George E. Pence

SEC to Up Its Enforcement Efforts

- New leadership at the SEC has made enforcement a renewed priority, one reflected in the fact that SEC brought more standalone enforcement actions during the past fiscal year than in the prior year. The Director of the SEC's Division of Enforcement Gurbir Grewal has indicated that the SEC will take a more aggressive approach to resolving investigations, including by seeking admissions of wrongdoing as part of its settlements with companies and by pursuing officer and director bars in more cases. As a recent example, in December 2021, the SEC and Commodity Futures Trading Commission (CFTC) announced settlements with a broker-dealer subsidiary of JP Morgan Chase & Co., in which the subsidiary agreed to pay \$200 million in fines and admitted to record-keeping violations related to its employees' use of personal devices and accounts to conduct company business. In announcing the settlements, the SEC revealed that it had opened other investigations of similar violations. The use of personal devices and accounts to conduct official business, which has long been the practice of many corporate board members, may have increased during the COVID-19 pandemic, with directors and employees working from home, increasingly reliant on electronic communications to do their work, and with the line between work and personal space becoming increasingly blurry.
- The SEC has also targeted violations associated with emerging technologies. In 2021, the SEC announced settlements concerning corporate disclosures around cyber incidents and reportedly conducted a sweep of cyber incident responses and

disclosures related to the SolarWinds cyber-attack. The SEC also announced settlements in several cryptocurrency-related cases covering various violations, including unregistered securities offerings. Corporate boards should expect these efforts to continue, especially in light of SEC Chair Gensler's August 2021 description of the asset class as "rife with fraud, scams and abuse." Gensler has also signaled his belief that the SEC may regulate many cryptocurrencies as securities under its remit.

- Rising SEC enforcement levels may have collateral consequences for companies, as admissions in SEC cases will boost private lawsuits filed by investors and other parties alleging wrongdoing by a company's directors or employees. Plaintiffs and their lawyers are likely to cite any admissions made to the SEC in their complaints. Corporate boards should therefore consider the risk of damages payouts in civil cases when deciding whether to enter any settlement with the SEC containing an admission of wrongdoing.

Prosecutors to "Be Bold" in Bringing Criminal Cases

- As 2021 came to a close, Deputy Attorney General Lisa Monaco, who oversees the DOJ's white-collar criminal cases, urged prosecutors to "be bold" in bringing those cases, raising the possibility that prosecutors may now move forward with cases that only a few years ago they would have declined. Deputy Monaco's public statements concerning prosecutions of executives at WorldCom, Qwest Communications, Adelphia, Tyco and Enron should give you a sense of the change of tone at the DOJ. Deputy Monaco also announced several DOJ policy changes that may impose greater burdens on corporate targets and lead to stiffer penalties for violations. They include increased disclosure obligations for corporations that are subject to investigation, a broader scope of past corporate misconduct that the DOJ will consider in resolving a criminal case, and the elimination of the presumption against using monitors to ensure a corporation's compliance with its remediation obligations.
- 2021 also saw the DOJ continue to focus on cybercrime. In October, the DOJ launched the Civil Cyber-Fraud Initiative targeting government contractors and grant recipients that provide deficient cybersecurity products or services, misrepresent their cybersecurity practices or protocols, or violate obligations to monitor and report cybersecurity incidents and breaches. The DOJ also ramped up its efforts to combat ransomware, citing the roughly \$350 million in ransom paid in 2020 alone as evidence of a growing national security threat. More attacks, and therefore payments made by victim companies, may be scrutinized by investigators. In addition to addressing the

business disruption caused by such attacks, corporate boards may have to decide whether to pay and report to the government any ransom payments. This decision may be complicated by recent Office of Foreign Assets Control (OFAC) guidance that a ransom payment made to a Specially Designated National or Blocked Person (SDN) may constitute a sanctions violation, subjecting the company to a range of penalties.

- Announced in November 2018, the DOJ's China Initiative includes the identification and resourcing of priority trade secret investigations and the development of an enforcement strategy concerning researchers in labs, universities and the defense industrial base that are allegedly transferring technology contrary to U.S. interests. Recently, the Initiative has suffered major setbacks, with prosecutors dropping charges in several cases and activists, the media and lawmakers arguing that the program harms the United States' research and technology competitiveness and raises concerns about racial profiling. Attorney General Merrick Garland said in October 2021 that the DOJ would review the department's approach to countering threats posed by the Chinese government, and the DOJ is reportedly expected to provide more information about the results of that review in the coming weeks. Even were the DOJ to abandon the China Initiative, new prosecutions arising from investigations that occurred during its lifetime may be just around the corner.
- Finally, the recent DOJ prosecution of Elizabeth Holmes, the founder and CEO of the now-defunct biotechnology company Theranos, should flag a sometimes overlooked risk of board service—reputational harm. In January 2022, a jury convicted Holmes on four counts of wire fraud. Media reports spotlighted the company's directors, many of whom were prominent names in government and finance, and suggested that they failed to provide an effective check on management's allegedly unlawful conduct.

Corporate Boards Should Take a Hard Look at Compliance Programs and Disclosures

- With key law enforcement posts in the Biden administration now filled, it is increasingly clear that the new sheriffs in town take a much grimmer view of alleged business misconduct than their predecessors. It remains to be seen whether their efforts will result in more successful enforcement actions, but at a minimum, corporate boards should expect investigations touching on the Biden administration's policy priorities, especially with respect to emerging technologies. To meet the increased risk of an enforcement event, corporate boards should review their

compliance programs and disclosures and, where necessary, commit additional resources to ensuring the company stays out of the SEC's and DOJ's crosshairs.

Categories

Corporate Governance

Board Governance

Compliance

© 2025 Akin Gump Strauss Hauer & Feld LLP. All rights reserved. Attorney advertising. This document is distributed for informational use only; it does not constitute legal advice and should not be used as such. Prior results do not guarantee a similar outcome. Akin is the practicing name of Akin Gump LLP, a New York limited liability partnership authorized and regulated by the Solicitors Regulation Authority under number 267321. A list of the partners is available for inspection at Eighth Floor, Ten Bishops Square, London E1 6EG. For more information about Akin Gump LLP, Akin Gump Strauss Hauer & Feld LLP and other associated entities under which the Akin Gump network operates worldwide, please see our Legal Notices page.