GT GreenbergTraurig

Alert | White Collar Defense & Special Investigations

March 2023

Clawbacks, Voluntary Disclosures, and Ephemeral Messaging: DOJ Continues Its Focus on Corporate Misconduct

Beginning in 2021, the U.S. Department of Justice has issued several policy memoranda and pronouncements setting forth factors federal prosecutors will consider when assessing corporate misconduct. On March 2-4, 2023, at the annual ABA National Institute on White Collar Crime, DOJ officials made a series of significant statements relating to the agency's current focus on alleged corporate wrongdoing. These policy initiatives will continue to create challenges and uncertainty for corporations.

In particular, Deputy Attorney General (DAG) Lisa Monaco announced DOJ's practice of encouraging clawbacks (i.e., money already paid out must be returned to the employer or the firm) and requiring compensation reforms as part of negotiated resolutions of criminal matters with corporations. At the same conference, Glenn Leon, chief of DOJ's Fraud Section, stated that DOJ expected to announce several criminal matters in the next several days that would provide clarity about what DOJ expects in terms of the timeliness and content of voluntary disclosures of corporate wrongdoing. David Last of DOJ's Foreign Corrupt Practices Act (FCPA) Section also offered further explanation of the voluntary disclosure program. This follows a recent policy memorandum by the DAG in February 2023 sent to all 93 U.S. Attorney's Offices with respect to voluntary disclosure by corporations. *See* Feb. 23 GT Alert. Lastly, Assistant Attorney General Kenneth Polite announced planned revisions to DOJ's Evaluation of Corporate Compliance Programs (ECCP) relating to the treatment of personal devices and ephemeral messaging services used by corporate employees, as well as clawbacks and compensation.

Clawback and Compensation Structures

DOJ is implementing a pilot program to encourage corporations to try to claw back compensation paid to individuals implicated in criminal wrongdoing. Under this policy, DOJ will reduce criminal fines corporations pay as part of a negotiated settlement if the company can show a good faith effort to claw back compensation, even if those efforts are unsuccessful. To be eligible, companies will need to demonstrate that:

- There is a clawback policy applicable to alleged criminal wrongdoing, including potentially for managers or supervisors who, though not directly a wrongdoer, turned a blind eye or failed to prevent wrongdoing by others; and
- Reasonable, good faith steps are being taken to effectuate the policy.

Further, in determining the amount of the fine reduction, prosecutors will consider the compensation clawed back at the time of resolution and potentially award up to a 25% reduction if the company is earnestly seeking or has sought to claw back compensation even if it has not received funds at the time of resolution. Under DOJ's policy, a company can keep the compensation that is successfully clawed back.

In addition, the DOJ's expected revisions to the ECCP will include directives to prosecutors to focus on corporations' compensation structures, particularly with an eye to whether they effectively reward compliance and/or punish or disincentivize wrongdoing, particularly where there are prior instances of alleged corporate misconduct. Highlighting this consideration of a company's compensation structures in relation to DOJ investigations and prosecutions, DAG Monaco pointed to DOJ's recent resolution with a financial institution where the entity agreed as part of the settlement to structure its compensation such that a failure to meet certain compliance benchmarks would result in no bonuses paid to executives.

'Immediate' Voluntary Disclosure of Misconduct

In February 2023, DOJ issued a formal policy memorandum to all U.S. Attorney's Offices providing guidance in prosecutions relating to voluntary disclosures of corporate wrongdoing. As explained in the memorandum, "Absent the presence of an aggravating factor, the USAO will not seek a guilty plea where a company has (a) voluntarily self-disclosed in accordance with the criteria set forth above, (b) fully cooperated, and (c) timely and appropriately remediated the criminal conduct." *See* Policy. One of the standards for a voluntary self-disclosure (VSD) consistent with the policy is that "[a] disclosure will only be deemed a VSD when the disclosure is made to the USAO …within a reasonably prompt time after the company becoming aware of the misconduct, with the burden being on the company to demonstrate timeliness." The FCPA's VSD policy provides a similar standard that "[t]he voluntary self-disclosure was made immediately upon the company becoming aware of the allegation of misconduct."

In response to questions and concerns about what DOJ means by a timely disclosure, the FCPA chief stated that DOJ will consider the facts and circumstances of each case but that prosecutors should consider the need for defense counsel to review the matters and ascertain the facts in order to advise the corporation. He also said that prosecutors should be mindful of the need for a company's management or board of directors to consider the effects of voluntary disclosure on the company. That said, DOJ cautioned that although a disclosure within weeks of the wrongdoing may be considered timely, an investigation that takes several months before there is a voluntary disclosure may not be considered as meeting DOJ's standard of immediacy. The practical application of this policy, and particularly the timeliness of the disclosure, is expected to be further revealed in a series of cases that DOJ intends to announce over the next several weeks and months.

Ephemeral Messaging and Personal Devices

Finally, DOJ also announced it would be updating its ECCP policy memorandum relating to the growing use of ephemeral messaging services and personal devices by corporate employees. Such services potentially hamper internal investigations and those law enforcement conduct as a result of lost data. Among other expected revisions, DOJ will consider corporate policies with respect to the use of ephemeral messaging and personal devices, particularly considering:

- Whether the company has adequately tailored its policies to the risks associated with the use of such services and the needs for data preservation and security; and
- How effectively the company communicates and enforces its policies, including data preservation needs, to its employees.

Additionally, DOJ will expect companies cooperating with law enforcement to readily answer questions regarding the companies' access to data on personal devices and the companies' policies regarding the same. If the company cannot produce such data, DOJ will expect companies to assist investigators in locating such data, acknowledging potential limitations under federal and state privacy laws. A company's declaration that it lacks knowledge about access to, or location of, data on personal devices or the prevalence of the use of ephemeral messaging by a company's employees will not suffice.

Implications and Considerations for Companies

DOJ remains focused on corporate conduct and is keen to see corporations take affirmative steps in their practices and policies to combat corporate wrongdoing and respond to instances of uncovered misconduct. These DOJ initiatives will pose substantial challenges to companies, particularly because many directly relate to corporate governance and policies. While previous DOJ policy updates have focused on punishing recidivists, incentivizing corporations to maintain substantial compliance programs and raising the specter of a new era of monitorships, the recently announced policies add a new dimension to the Department's approach to combatting corporate crime – DOJ is now looking to crack down on corporate pocketbooks and the use of encrypted communications platforms.

For example, company policies regarding clawbacks and compensation structures tied to compliance are complex questions implicating a host of legitimate business considerations, including recruitment and retention. Further, the ability to claw back compensation paid to former employees may be legally and factually formidable. It remains to be seen to what extent DOJ will require clawback attempts that a company might ordinarily not pursue due to legal obstacles. Similarly, it remains to be determined how widely DOJ will expect clawback efforts for those not directly responsible for misconduct, and what a company must show as evidence of good faith efforts to claw back compensation.

Considerations of corporate employees' use of ephemeral messaging services or bring your own device (BYOD) policies already pose complicated decisions for companies. DOJ's expected revisions to its ECCP, with a focus on data preservation and accessibility, further adds to the factors companies will need to consider with respect to data and communications policies, as well as how much cooperation a company can reasonably provide given state privacy laws.

And with respect to the timing of voluntary disclosures, questions still exist regarding how a company must balance DOJ's policy of a timely disclosing wrongdoing—particularly if that means within a few weeks of discovery—and a company's legitimate business need to sufficiently learn the extent of wrongdoing and consider the effects on its business, including with regulators, strategic partners, and investors. In-house counsel, practitioners, and prosecutors alike will eagerly look to upcoming DOJ announcements regarding criminal matters relating to voluntary disclosure as practical applications of DOJ's voluntary disclosure policy.

In the meantime, there are several steps a company can consider taking:

Clawback and Compensation Policies: Companies should consider taking a hard look at their existing policies regarding clawbacks and how compensation is structured in connection with alleged wrongdoing. If companies do not have such policies in place, they should consider whether such policies are appropriate given the companies' legitimate business needs and the potential for criminal exposure. If a company already has clawback and compensation policies in place, it should consider how effective they are, particularly in terms of clawing back compensation from former employees, whether they permit clawback from those not directly implicated in the wrongdoing but who may have failed to reasonably detect or prevent malfeasance, and whether the compensation structure provides a reasonable range of carrots for compliance and sticks to disincentivize wrongdoing.

Ephemeral Messaging and BYOD Policies: In formulating or revising policies regarding the use of ephemeral messaging services by employees and/or BYOD, companies should consider, among other business considerations, the availability of the data in the event of an investigation, whether internal or by law enforcement. If a company has a BYOD policy or allows certain ephemeral messaging services, it should also consider data-preservation requirements for employees, at least with respect to certain information, and how effectively those policies are communicated. And counsel needs to be knowledgeable about these policies and the accessibility and location of third-party data before negotiating with DOJ.

Voluntary Disclosure: Companies should consider having an operational plan in place setting forth specific steps to take in response to any allegations of wrongdoing. Steps could include having established procedures for conducting interviews; policies and infrastructure to allow for quick review of company electronically stored information (ESI), including employee data; and ready lines of communication with or between internal and external individuals necessary for an effective investigation, such as representatives of management, in-house counsel, IT, HR, and possibly outside experienced criminal counsel. This will better position a company to quickly ascertain the potential scope of wrongdoing, at least preliminarily, so that the company can then take any required internal steps to evaluate when and whether to voluntarily disclose the wrongdoing to DOJ and/or the appropriate regulatory or investigative entity.

As companies know, there is rarely a one-size-fits-all approach. But given DOJ's policy pronouncements as part of its current focus on corporate misconduct, most companies will be well-served to take them into account in evaluating existing policies.

Authors

This GT Alert was prepared by the following attorneys on behalf of the firm's White Collar Defense & Special Investigations Practice:

- Todd A. Pickles | +1 916.868.0628 | picklest@gtlaw.com
- Benjamin G. Greenberg | +1 305.579.0850 | greenbergb@gtlaw.com
- Kyle R. Freeny | +1 202.331.3118 | freenyk@gtlaw.com
- John Huber | +1 801.478.6915 | John.Huber@gtlaw.com
- Mark J. Lesko | +1 631.994.2408 | Mark.Lesko@gtlaw.com