GT GreenbergTraurig

Alert | White Collar Defense & Special Investigations

March 2019

DOJ Eases Stance on Use of Disappearing Message Platforms in Corporate Enforcement Policy

On March 8, 2019, the Department of Justice announced changes to the Foreign Corrupt Practice Act's (FCPA) Corporate Enforcement Policy prohibiting the use of disappearing message platforms. The DOJ eliminated a policy that some interpreted as requiring companies to internally ban common disappearing message platforms. Historically, many banks have prohibited the use of disappearing message platforms, but the change to DOJ policy now permits companies to use such platforms to the extent the companies comply with certain measures. The amended policy recognizes the current prevalence of such message platforms and the likelihood of future advancements in the technology. The amended policy also makes other changes discussed below.

Prior to implementation of the new DOJ policy change, the business community was concerned with the practicality of enforcing a ban on disappearing message platforms and prohibiting employees from using software that generates, but does not appropriately retain, business records or communications. DOJ's FCPA Corporate Enforcement Policy, which continues to encourage self-reporting of suspected bribes, removes the outright prohibition of disappearing message platforms and replaces it with new controls on such communication methods.

Specifically, the amended policy requires that companies implement "appropriate guidance and controls on the use of personal communications and ephemeral messaging platforms that undermine the company's ability to appropriately retain business records or communications or otherwise comply with the company's document retention policies or legal obligations." JM 9-47.120(3). Companies now have

more flexibility to choose the technology and compliance system that tailors best to their business needs. Among other things, companies should consider whether to institute use of enterprise versions of the message platforms designed to retain messages or invest in technology to otherwise preserve relevant data in accordance with appropriate records retention policies, and provide guidance to employees regarding how such message platforms are permitted to be used for types of work or personal matters.

There are several additional noteworthy changes to the corporate enforcement policy that corporations should be aware of. First, one change addresses the practice of de-confliction, which occurs when prosecutors ask corporate counsel to refrain from interviewing an employee of an internal investigation because DOJ would like to talk to them first. The amended policy now clarifies that DOJ will not take any steps to affirmatively direct a company's internal investigation efforts, although it keeps intact DOJ's ability to make de-confliction requests of a company. This policy change resulted from two cases in which defendants claimed their employers were indirect extensions of the government, impacting the course of the government's investigations and the employees' rights. A second amendment makes the policy applicable to companies undergoing mergers or acquisitions. Companies can now avail themselves of the corporate enforcement policy if they find wrongdoing at a company they are acquiring, voluntarily self-disclose the misconduct, and take the necessary corrective actions. Third, the policy clarifies that companies need not waive attorney-client privilege to get cooperation or self-reporting credit.

These amendments follow other important recent revisions to DOJ's Corporate Enforcement Policy. One recent policy change intended to alleviate difficulties companies faced in self-reporting allows companies to turn over to the government all relevant facts on individuals if they were "substantially involved," rather than the previous policy that was potentially much broader by requiring information to be disclosed on all individuals who were "involved" in any violations.

Now that the revised DOJ policy regarding disappearing message platforms is in place, there are important considerations that companies must consider moving forward. First, the amended policy provides employers with the freedom to alter their technology systems regarding ephemeral message apps, provided there is proper compliance. However, employers must evaluate how much policing is needed to ensure employees are not using these apps for inappropriate reasons or without retaining necessary records. Obviously, the use of disappearing message platforms could render potentially relevant evidence lost forever. It is up to companies to decide whether an outright ban on disappearing message systems best fits their needs, or if they wish to take advantage of the newly amended policy. If companies do wish to take advantage of this policy change, then they must upgrade their compliance programs to account for these messaging technologies. Employers should institute adequate policies and procedures that account for the use of these messaging platforms and should ensure employees are able to comply with necessary records retention requirements.

Authors

This GT Alert was prepared by **Daniel P. Filor, Nathan J. Muyskens, Jessica Natali**, and **Robert W. Rubenstein**. Questions about this information can be directed to:

- Daniel P. Filor | +1 212.801.6758 | filord@gtlaw.com
- Nathan J. Muyskens | +1 202.331.3164 | muyskensn@gtlaw.com
- Jessica Natali | +1 215.988.7824 | natalij@gtlaw.com
- Robert W. Rubenstein | +1 215.988.7846 | rubensteinr@gtlaw.com
- Or your Greenberg Traurig attorney

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