COVINGTON

DOJ Revises FCPA Corporate Enforcement Policy

April 3, 2019

Anti-corruption/FCPA

In March 2019, the U.S. Department of Justice introduced several changes to the Foreign Corrupt Practices Act ("FCPA") Corporate Enforcement Policy ("the Policy"). The Policy, originally incorporated into the Justice Manual in November 2017, outlines the Department's position on mitigation credit that companies may receive for voluntary self-disclosure, full cooperation, and timely and appropriate remediation in FCPA matters. Since 2018, the Criminal Division of DOJ has been using the Policy as guidance outside of the FCPA context.

Most of the changes to the Policy formalize previously announced guidance or reflect recent Department practices. Two of the changes to the Department's written position on remediation and cooperation are particularly notable:

- First, in order to be eligible to receive full credit for timely and appropriate remediation, companies are required to implement "appropriate guidance and controls" on employees' use of personal communications and ephemeral messaging systems. This revision walks back the Department's previous position that full remediation credit required a prohibition on the use of "software that generates but does not appropriately retain business records or communications."
- Second, the revised Policy establishes a presumption of a declination for a company in a merger or acquisition transaction where the company voluntarily discloses misconduct uncovered in pre-acquisition due diligence or post-acquisition integration, as long as the company meets certain other requirements outlined in the Policy. This revision formalizes a practice DOJ announced in July 2018.

In addition, the Policy reflects a previously announced position on the disclosure of individual involvement in misconduct. As Deputy Attorney General Rod Rosenstein announced in November 2018, companies are only required to identify individuals "substantially involved in or responsible for the misconduct," instead of "all individuals involved in or responsible for the misconduct," in order to receive cooperation credit. In recent comments, Deputy Assistant Attorney General Matthew Miner further clarified that in order to get some cooperation credit, companies needed only to provide evidence on individuals "substantially involved," but that in order to get full cooperation credit, the Department would expect more.

The Policy also clarifies that de-confliction requests by the Department must be "appropriate." De-confliction requests arise when the DOJ asks a company to defer an investigative step—typically, interviewing employees—until after the government has an opportunity to do so. Both in public comments and in our interactions with DOJ, we have raised concerns that de-confliction requests can put company directors and officers in a challenging position, in which their ability to conduct an investigation and take remedial action expeditiously (which may be

necessary to discharge their fiduciary duties) can be in tension with a desire to accede to DOJ's request. Under the revised Policy, de-confliction is one factor that the Department may consider in "appropriate cases" in determining the extent of cooperation credit. Furthermore, the Policy confirms that the Department will not take any steps to "affirmatively direct a company's internal investigation efforts."

Finally, the Policy reaffirms that eligibility for self-disclosure credit is not predicated upon the waiver of attorney-client privilege or work product protection.

We explore the details of the notable changes to the Policy below.

Ephemeral Messaging

The Policy revisions with respect to ephemeral messaging platforms come on the heels of a flurry of questions and concerns from companies after the announcement of the 2017 Policy. Under the 2017 Policy, to receive credit for "appropriate remediation," companies were required to "prohibit[] the improper destruction or deletion of business records, including prohibiting employees from using software that generates but does not appropriately retain business records or communications." As we noted in our 2018 Year in Review, despite this strict language, DOJ officials later indicated that the Department did not necessarily expect companies to impose outright prohibitions on the use of such messaging applications. Instead, companies should take a "risk-based approach" and be able to explain to DOJ what steps they have taken with respect to the use of messaging applications, and why. The recent Policy revisions appear to formalize the Department's endorsement of a risk-based approach to ephemeral messaging platforms.

Under the revised Policy, companies that wish to preserve their ability to obtain full remediation credit must implement "appropriate guidance and controls on the use of personal communications and ephemeral messaging platforms." The Policy does not provide any detail on what constitutes "appropriate guidance and controls." While companies may take some comfort in the removal of a blanket prohibition of ephemeral communication applications, in practice, prosecutors applying the Policy will have considerable discretion in determining whether a company has put in place guidance and controls that are "appropriate."

Given the shift to a risk-based approach for ephemeral messaging platforms, we think companies should consider undertaking a holistic communications risk assessment to enable the development of tailored policies and controls. Critically, the legal considerations for such a risk assessment are not limited to preserving arguments for remediation credit under the Policy; in certain cases, gaps in data retention policies and practices could expose companies to scrutiny for inadequate internal accounting controls, spoliation of evidence, or, in extreme cases, obstruction of justice. As part of a communications risk assessment, companies could take the opportunity to critically assess the strengths and weaknesses of the organization's broader data retention and information governance policies and procedures.

Transactional Due Diligence and Integration

The expansion of the Policy to cover transactional compliance due diligence and integration represents the DOJ's most significant policy statement on mergers or acquisitions activities since the publication of the FCPA Resource Guide in 2012. The Resource Guide stated that DOJ "may" decline to bring enforcement actions against successor companies that undertake certain M&A best practices and voluntarily disclose misconduct. The revised Policy provides greater certainty for companies by establishing a "presumption of declination" when companies

(i) uncover misconduct through thorough and timely due diligence or through post-acquisition audits or compliance integration efforts, (ii) voluntarily disclose the misconduct, and (iii) otherwise take action consistent with the Policy, such as timely implementing an effective compliance program at the merged or acquired entity. Importantly, a footnote in the Policy makes clear that "[i]n appropriate cases, an acquiring company that discloses misconduct may be eligible for a declination, even if aggravating circumstances existed as to the acquired entity."

As Deputy Assistant Attorney General Matthew Miner made clear when this policy change was first announced in July 2018, DOJ's goal is to not discourage "law-abiding companies with robust compliance programs" from acquiring non-compliant companies. DOJ explained in September 2018 that these principles will apply in the merger and acquisition context when other types of wrongdoing—not just FCPA violations—are uncovered. As we previously noted, while not game-changing, this policy change clarified that acquiring entities may receive the benefit of disclosure even in situations where the selling or acquired company was aware of the improper conduct prior to the transaction.

Since Deputy Assistant Attorney General Miner's announcement, commentators have welcomed the increased clarity on DOJ's position with respect to corruption issues identified in the course of M&A transactions, an area that can be fraught with risk. However, DOJ's position may not significantly alter the risk calculus for companies assessing whether to voluntarily disclose corruption issues identified in the course of M&A transactions. Although the prospect of a declination or substantial fine reduction will naturally be appealing to an acquirer that identifies potential FCPA issues, there are a number of countervailing considerations that should be evaluated in assessing whether to make a voluntary disclosure to DOJ.

- First, though the Policy offers increased certainty with respect to the availability of a declination, DOJ has continued to reserve some discretion for itself under the "aggravating circumstances" exception, which may be invoked on the basis of a relatively broad list of factors, including involvement by executive management in the misconduct, a significant profit arising from the misconduct, the pervasiveness of the misconduct within the company, and criminal recidivism. It is not clear from the face of the Policy what "appropriate cases" involving aggravating circumstances would qualify for a declination.
- Second, a disclosure to DOJ may result in a referral to the SEC or enforcement authorities in other jurisdictions, which are not bound by the Policy and may take action even where DOJ declines to prosecute.
- Third, declinations under the Policy are likely to be accompanied by disgorgement. Nearly all of the declinations issued under the Pilot Program and the 2017 Policy have involved disgorgement, either to the SEC or to DOJ. Notably, any financial penalties incurred by an acquirer may be in addition to financial losses resulting from the over-valuation of a target company that derived a portion of its profits from corrupt conduct.
- Finally, the Policy's focus on the "acquiring entity" leaves some ambiguity as to whether a target company that continues to exist following an acquisition will benefit from a declination under the Policy along with the acquirer. There have been a number of instances in which DOJ declined to pursue an enforcement action against an acquirer that uncovered and remediated misconduct, but nonetheless pursued an action against the acquired entity. Indeed, the Resource Guide indicates that DOJ and SEC have only taken action against successor companies in limited circumstances and that they have

more often pursued actions against acquired entities.[1] Although it is undoubtedly a preferable result from an acquirer's standpoint for an action to be brought against the acquired entity rather than the acquirer itself, an action against an acquired business may nonetheless result in a substantial loss of value in the investment or otherwise impact the acquirer's business.

If you have any questions concerning the material discussed in this client alert, please contact the following members of our Anti-corruption/FCPA practice:

Lanny Breuer	+1 202 662 5674	lbreuer@cov.com
Eric Carlson	+86 21 6036 2503	ecarlson@cov.com
Sarah Crowder	+44 20 7067 2393	scrowder@cov.com
Steven Fagell	+1 202 662 5293	sfagell@cov.com
Mark Finucane	+1 202 662 5601	mfinucane@cov.com
James Garland	+1 202 662 5337	jgarland@cov.com
Ben Haley	+27 (0) 11 944 6914	bhaley@cov.com
Nancy Kestenbaum	+1 212 841 1125	nkestenbaum@cov.com
Mona Patel	+1 202 662 5797	mpatel@cov.com
Mythili Raman	+1 202 662 5929	mraman@cov.com
Don Ridings	+1 202 662 5357	dridings@cov.com
Jennifer Saperstein	+1 202 662 5682	jsaperstein@cov.com
Daniel Shallman	+1 424 332 4752	dshallman@cov.com
Phoebe Yu	+1 202 662 5939	pyu@cov.com

This information is not intended as legal advice. Readers should seek specific legal advice before acting with regard to the subjects mentioned herein.

Covington & Burling LLP, an international law firm, provides corporate, litigation and regulatory expertise to enable clients to achieve their goals. This communication is intended to bring relevant developments to our clients and other interested colleagues. Please send an email to unsubscribe@cov.com if you do not wish to receive future emails or electronic alerts.

[1] Resource Guide at 28–30.