

Regulatory Alert

Regulatory Insights

March 2023

DOJ Initiatives on Compensation, Voluntary Self-Disclosure, Personal Devices

KPMG Regulatory Insights:

- *The DOJ's initiatives related to compensation, voluntary self-disclosure, and personal devices showcase the ongoing focus across regulators and enforcement agencies on accountability, including companies' efforts to cooperate, remediate misconduct, and provide incentives for ethical behavior.*
- *The DOJ's actions build off the "Monaco Memo" (see KPMG Regulatory Alert, [here](#)), by piloting a program on incentives/clawbacks for individuals "responsible for misconduct" and promoting self-disclosure of issues to regulators/prosecutors before "imminent threat" of public disclosure or government investigation.*
- *Concurrently, DOJ has announced it will be hiring 25 new prosecutors within its National Security Division as well as making a "substantial investment" within the Criminal Division, setting forth expectations for additional investigations/actions.*

Pursuant to the Deputy Attorney General's September 2022 memorandum (Monaco Memo – see KPMG's Regulatory Alert, [here](#)), as well as the DOJ Criminal Division's recent revision of its Corporate Enforcement Policy (see KPMG's Regulatory Alert, [here](#)), the DOJ recently announced initiatives that reinforce the agency's continuing focus on corporate compliance, enforcement, and accountability:

- Launch of a pilot program on compensation incentives and clawbacks
- Implementation of a voluntary self-disclosure (VSD) policy
- Changes to the Evaluation of Corporate Compliance Program (ECCP) regarding the use of personal devices
- Commitment to additional resources

These announcements are outlined in further detail below.

Pilot Program on Compensation Incentives and Clawbacks

The DOJ's Criminal Division announced it will launch a three-year [pilot program](#), beginning March 15, on Compensation Incentives and Clawbacks. The program was developed giving consideration to how policies might seek to potentially "shift the burden of corporate wrongdoing away from shareholders—who frequently play no role in misconduct—onto those more directly responsible," as well as to reward companies that incentivize compliance through compensation programs. The pilot program consists of two parts:

- First, every corporate resolution involving the Criminal Division will now include a requirement that the resolving company develop compliance-promoting criteria within its compensation and bonus system and, during the term of the resolution, report annually on the

implementation of the criteria. These criteria may include, but are not limited to:

- A prohibition on bonuses for employees who do not satisfy compliance performance requirements.
 - Disciplinary measures for employees who violate applicable law and others who both (a) had supervisory authority over the employee(s) or business area engaged in the misconduct and (b) knew of, or were willfully blind to, the misconduct.
 - Incentives for employees who demonstrate full commitment to compliance processes.
- Second, the Criminal Division will consider possible fine reductions up to 100 percent of recouped compensation for companies that “fully cooperate”, “timely and appropriately” remediate misconduct, and demonstrate they have implemented a program to claw back compensation from employees who engaged in wrongdoing in connection with the conduct under investigation, or others who both (a) had supervisory authority over the employee(s) or business area engaged in misconduct and (b) knew of, or were willfully blind to, misconduct. Further, the process to recoup such compensation must have been initiated in good faith before the time of resolution.
- If the company’s good faith effort fails to recoup compensation, DOJ may still consider possible fine reductions of up to 25 percent of the amount of compensation the company attempted to claw back, depending on the circumstances.

Voluntary Self-Disclosure Policy

The DOJ’s United States Attorneys’ Offices (USAOs) [announced](#) the implementation of a new VSD policy.

DOJ states the policy is intended to provide “transparency and predictability” to companies by standardizing how VSDs are defined and credited by USAOs nationwide, and to incentivize companies to maintain effective compliance programs capable of timely identification, voluntary self-disclosure, and remediation of misconduct, as well as full cooperation with the government in corporate criminal investigations.

The policy, which is effective immediately, outlines the circumstances under which a company will be considered to have made a VSD of misconduct to a USAO.

Standards. A company will be required to meet each of the following standards:

- **Voluntary:** Disclosure of misconduct must be made voluntarily by the company, and not where there is a preexisting obligation to disclose, such as regulation,

contract, or a prior Department resolution (e.g., non-prosecution agreement or deferred prosecution agreement).

- **Timely:** Disclosure to the USAO must be made:
 - Prior to an imminent threat of disclosure or government investigation.
 - Prior to the misconduct being publicly disclosed or otherwise known to the government.
 - Within a “reasonably prompt” time after a company becomes aware of the misconduct, with the burden being on a company to demonstrate timeliness.
- **Substance:** Disclosure must include all relevant facts concerning the misconduct that are known to a company at the time of the disclosure.

Benefits. A company that provides a VSD and meets the other requirements of the policy, involving full cooperation and timely remediation of criminal conduct (including, but not limited to, agreeing to pay all disgorgement, forfeiture, and/or restitution resulting from the misconduct), and in the absence of any aggravating factor (outlined below), will receive credit for the VSD and “significant” benefits, including the USAO not:

- Seeking a guilty plea.
- Choosing to impose any criminal penalty.
- Imposing a criminal penalty that is greater than 50 percent below the low end of the U.S. Sentencing Guidelines (USSG) fine range.
- Seeking the imposition of an independent compliance monitor if the company demonstrates that it has implemented and tested an effective compliance program.

Aggravating Factors. The policy identifies three aggravating factors that may warrant a USAO seeking a guilty plea or criminal penalties, even if the other requirements of the VSD policy are met. These include situations where the misconduct:

- Poses a grave threat to national security, public health, or the environment.
- Is deeply pervasive throughout the company.
- Involved current executive management of the company.

The policy notes that the presence of an aggravating factor does not necessarily mean that a guilty plea will be required, rather the USAO may assess the relevant facts and circumstances to determine the appropriate resolution. If a guilty plea is required, a company may still receive the other benefits under the VSD policy, including the USAO recommending a criminal penalty of at least 50 to 75 percent

reduction off the low end of the USSG fine range and not requiring the appointment of a monitor if a company has implemented and tested an effective compliance program.

Effective Compliance and Independent Monitorship. As stated above, the USAO will not require the imposition of an independent compliance monitor if a company demonstrates it has implemented and tested an effective compliance program. These decisions will be made on a case-by-case basis and at the sole discretion of the USAO. In evaluating the adequacy of a company's compliance program, the USAO will refer to the "Monaco Memo" (which provides "a mix of incentives and deterrence" to enhance corporate compliance in areas such as individual accountability, history of misconduct, VSD, independent compliance monitors, and corporate culture), in addition to other resources developed by DOJ's Criminal Division to assist in assessing the effectiveness of a company's compliance program as well as guidance provided by other DOJ Divisions as to specialized areas of corporate compliance.

ECCP Changes for Personal Devices

The Assistant Attorney General [announced](#) changes to the ECCP regarding how DOJ will consider a company's "approach to the use of personal devices as well as various communications platforms and messaging applications, including those offering ephemeral messaging." In particular, DOJ will consider:

- How policies are tailored to a company's risk profile and business needs, as well as how the policies are communicated to employees and how they are enforced.

- Whether business-related electronic data and communications can be preserved and accessed as well as deletion policies/settings, including through any "bring-your-own-device" programs.

(See related KPMG Regulatory Alert, [here](#), on increasing regulatory expectations for data retention and deletion.)

Additional Resources

DOJ [announced](#) new resource commitments and a restructuring of its National Security Division to address "the intersection of corporate crime and national security" by adding more than 25 new prosecutors to investigate and prosecute sanctions evasion, export control violations, and similar economic crimes. With regard to corporate sanctions violations, the National Security Division will work closely with U.S. Attorneys' Offices and the Criminal Division. Concurrently, the Criminal Division intends to make a "substantial investment" into its Bank Integrity Unit (part of the Money Laundering and Asset Recovery Section) to strengthen prosecutions of global financial institutions for sanctions violations.

For more information, please contact [Amy Matsuo](#), [Marc Miller](#), or [Matt McFillin](#).

Contact the author:



Amy Matsuo
Principal and National
Leader
Regulatory Insights
amatsuo@kpmg.com

kpmg.com/socialmedia



Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

All information provided here is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the facts of the particular situation.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.