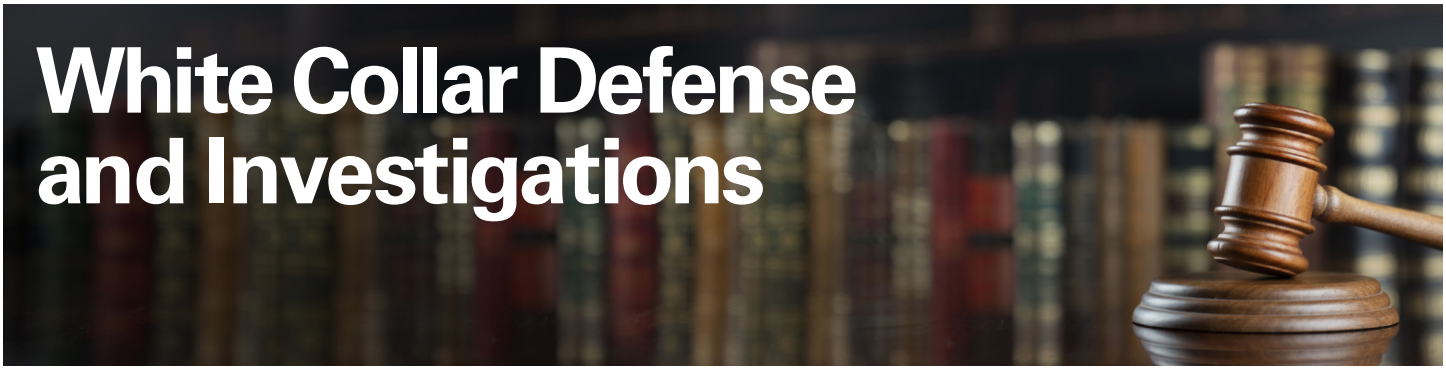
March 10, 2023

Skadden

White Collar Defense and Investigations



If you have any questions regarding the matters discussed in this memorandum, please contact the attorneys listed on the last page or call your regular Skadden contact.

One Manhattan West
New York, NY 10001
212.735.3000

DOJ Focus on Corporate Enforcement Continues With Updated Policies Related to Corporate Crime and Compliance Programs

In early March 2023, the Department of Justice (DOJ) released several important updates to its policies related to corporate crime enforcement and compliance programs. We discuss below the following key topics:

> (i) The DOJ is encouraging corporate entities to (a) update compliance programs with performance and evaluation systems that tie compliance to compensation incentives or deterrents and (b) consider financial penalties as part of the consequences for employee misconduct. Notably, the DOJ has announced it will require all entities entering into a criminal resolution to implement compliance-related criteria as part of their compensation systems.
>
> (ii) The DOJ expects companies to implement risk-based and properly developed policies and procedures governing employees' use of personal devices and messaging applications to ensure preservation of and access to business-related data and communications.
>
> (iii) The DOJ has clarified the factors it will consider in deciding whether to impose an independent compliance monitor as part of a criminal corporate resolution. These include, for example, whether an entity has made relevant changes to its corporate culture and leadership, fully remediated, and implemented and tested an effective and well-resourced compliance program.

DOJ Seeks To Tie Compensation Incentives to Compliance

New ECCP Guidelines

The updated Evaluation of Corporate Compliance Program (ECCP) guides prosecutors to consider as part of their charging and resolution decisions the following factors, among others, in evaluating whether an entity has implemented a compensation system that promotes compliance:

- Whether the company publicizes disciplinary actions related to compliance misconduct internally, where appropriate and possible to deter future misconduct.
- Whether the company tracks data relating to disciplinary actions in order to measure the effectiveness of the investigation and consequence management functions (*e.g.*, by monitoring the number of substantiated allegations, average time to complete an investigation, and effectiveness and consistency of disciplinary measures across the company).

- Whether the company has incentivized compliance by designing compensation systems that (a) defer or escrow certain compensation tied to conduct consistent with company values and policies or (b) permit the company to recoup previously awarded compensation if an individual is found to have engaged in wrongdoing.
- Whether the company maintains and enforces the provisions for recoupment or reduction of compensation due to compliance violations or misconduct.
- Whether the company has tested the effectiveness of its disciplinary and compensation structure, for example, by analyzing hotline report data.

Pilot Program

In addition, the DOJ's Criminal Division has launched a three-year pilot program that seeks to encourage companies to factor compliance into their compensation and bonus structures as a way to promote compliance culture. The pilot program comes into effect on March 15, 2023, and at the end of the three-year pilot period, the Criminal Division will assess whether to extend or modify the program.

The pilot program has two parts. First, going forward, every corporate resolution the Criminal Division enters into will require the company to implement compliance-related criteria in its compensation and bonus system and to report annually to the Criminal Division about that implementation during the term of such resolutions. Compliance-related criteria may include, for example, (i) a prohibition on bonuses for employees who do not satisfy compliance performance requirements; (ii) disciplinary measures for employees who violate applicable law and others who have supervisory authority over the employees or business area involved in the misconduct and who knew of (or were willfully blind to) the misconduct; and/or (iii) incentives for employees who demonstrate commitment to compliance. This requirement was applied in the recent Danske Bank resolution, which we discussed in a December 16, 2022, client alert "Key Takeaways From Danske Bank's Settlement of DOJ and SEC Fraud Charges Over Its Anti-Money Laundering Compliance."

Second, the Criminal Division will consider fine reductions where companies seek to recoup compensation from employees who engaged in misconduct. Under the pilot program, prosecutors may accord a reduction of the fine in the amount of 100% of any compensation that a company is able to recoup during the period of the resolution. Companies may also receive a reduction for good faith attempts to recoup compensation.

Use of Personal Devices and Messaging Platforms

As anticipated, the ECCP also provides additional guidance to prosecutors in the program on evaluating corporate policies regarding employees' use of personal devices and third-party messaging platforms.

Going forward, prosecutors will evaluate, as part of charging and resolution decisions, the following issues:

- Whether a company's policies on the use of personal devices and messaging applications are (a) tailored to the corporation's risk profile and specific business needs and (b) communicated consistently to employees.
- Whether those policies ensure that, as appropriate, the company can preserve and access business-related electronic data and communications.
- Whether the company enforces its preservation and access policies consistently (*e.g.*, imposes consequences on employees who refuse to grant the company access or has exercised its rights or disciplined employees who fail to comply with retention and access policies).
- Whether employees use electronic communication channels to conduct business and whether such channels have archival and preservation settings.
- Whether the company has a "bring your own device" (BYOD) program and, if so, how it works to ensure data preservation. Enforcers will consider, for example:
  - The company's policies governing preservation of and access to corporate data and communications stored on personal devices — including data on messaging platforms — and the rationale behind those policies.
  - If the policies permit the company to review business communications on BYOD or messaging apps.
  - What exceptions or limitations to these policies have been permitted.
  - If the company's approach seems reasonable given its business needs and risk profile.
- During an investigation, if a company has not produced communications from third-party messaging applications, prosecutors will ask about the company's ability to access such communications, whether they are stored on corporate devices or servers, as well as applicable privacy and local laws, among other things.

Assistant Attorney General Kenneth Polite noted in announcing these policy updates that "a company's answers — or lack of answers — may very well affect the offer it receives to resolve criminal liability."

Consistent with these updates, companies should expect the DOJ to investigate policies governing preservation of and access to corporate data and communications stored on personal devices

(including data on messaging platforms). Companies should consider evaluating their policies regarding permissible use of mobile devices and messaging platforms, particularly those relating to BYOD programs. Going forward, companies will not be able to avoid the DOJ's preservation and disclosure expectations because employees use their own devices or conduct business on third-party messaging apps that do not preserve data.

Updated Guidance on Selection of Monitors in Criminal Division Matters

Finally, Assistant Attorney General Polite issued a revised memorandum on selection of monitors in Criminal Division matters (the Polite Memorandum), supplementing prior memoranda issued by former Acting Deputy Attorney General Craig Morford in 2008 (the Morford Memorandum) and former Assistant Attorney General Brian Benczkowski in 2018 (the Benczkowski Memorandum). The Polite Memorandum clarifies how the Criminal Division will determine whether a corporate monitor is appropriate as part of a corporate criminal resolution.

The Polite Memorandum instructs prosecutors not to apply presumptions for or against monitors. Instead, in assessing the need for and potential benefits of a monitor, the DOJ may broadly consider whether an entity has made relevant changes to corporate culture or leadership and taken effective remedial actions, including implementation of an effective, adequately tested and resourced compliance program.

More specifically, the memo directs prosecutors to consider a list of ten nonexhaustive factors:

1. Whether the corporation met voluntary self-disclosure requirements. (See our March 3, 2023, client alert "DOJ Implements Voluntary Self-Disclosure Policy for US Attorneys' Offices" on the requirements and expectations for voluntary self-disclosures.)
2. Whether, at the time of the resolution and after a thorough risk assessment, the corporation has implemented an effective compliance program and sufficient internal controls to detect and prevent similar misconduct in the future.
3. Whether, at the time of the resolution, the corporation has adequately tested its compliance program and internal controls to demonstrate that they would likely detect and prevent similar misconduct in the future.
4. Whether the underlying criminal conduct was long-lasting or pervasive across the business organization or was approved, facilitated or ignored by senior management, executives or directors (including by means of a corporate culture that tolerated risky behavior or misconduct or that did not encourage open discussion and reporting of possible risks and concerns).
5. Whether the underlying criminal conduct involved the exploitation of an inadequate compliance program or system of internal controls.
6. Whether the underlying criminal conduct involved active participation of compliance personnel or the failure of compliance personnel to appropriately escalate or respond to red flags.
7. Whether the corporation took adequate investigative or remedial measures to address the underlying criminal conduct.
8. Whether, at the time of the resolution, the corporation's risk profile has substantially changed such that the risk of recurrence of the misconduct is minimal or nonexistent.
9. Whether the corporation faces any unique risks or compliance challenges (*e.g.,* due to its region or business sector).
10. Whether and the extent to which the corporation is subject to oversight from industry regulators or is receiving a monitor from another domestic or foreign enforcement authority or regulator.

The Polite Memorandum also clarifies that many of the requirements for monitors apply to entire monitor teams, not just to lead monitors, and that the DOJ will select and assign monitors in alignment with its commitment to diversity, equity and inclusion. Finally, pursuant to the Polite Memorandum, the cooling-off period for monitors (*i.e.*, the time after the monitorship where the monitor cannot represent the company on additional matters) is now at least three years (rather than two years) from the date of the termination of the monitorship.

* * *

DOJ officials have made clear that upcoming resolutions will reflect the updated policies, including the recent updates to the Criminal Division's and U.S. Attorney's Offices' voluntary self-disclosure requirements and expectations.

In particular, companies and financial institutions should consider reviewing their compliance programs with respect to compensation systems and the use of personal devices and messaging applications. Companies should consider carefully documenting the business-related and risk-based factors they used in developing those programs, how the policies are effectively communicated to employees, the training employees undergo on the policies, and the testing and consistent enforcement of such policies.

DOJ Implements Voluntary Self-Disclosure Policy for US Attorneys' Offices

Contacts

Jennifer L. Bragg
Partner / Washington, D.C.
202.371.7980
jennifer.bragg@skadden.com

Maria Cruz Melendez
Partner / New York
212.735.2320
maria.cruzmelendez@skadden.com

Jack P. DiCanio
Partner / Palo Alto
650.470.4660
jack.dicanio@skadden.com

Alessio Evangelista
Partner / Washington, D.C.
202.371.7170
alessio.evangelista@skadden.com

Maya P. Florence
Partner / Boston
617.573.4805
maya.florence@skadden.com

Steven R. Glaser
Partner / New York
212.735.2465
steven.glaser@skadden.com

Andrew M. Good
Partner / London
44.20.7519.7247
andrew.good@skadden.com

Christopher J. Gunther
Partner / New York
212.735.3483
christopher.gunther@skadden.com

Ryan D. Junck
Partner / London
44.20.7519.7006
ryan.junck@skadden.com

Steve Kwok
Partner / Hong Kong
852.3740.4788
steve.kwok@skadden.com

David Meister
Partner / New York
212.735.2100
david.meister@skadden.com

Bora P. Rawcliffe
Counsel / London
44.20.7519.7139
bora.rawcliffe@skadden.com

Zaneta Wykowska
Associate / London
44.20.7519.7129
zaneta.wykowska@skadden.com