

# Government Enforcement and White Collar Crime Alert



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.

This memorandum is provided by Skadden, Arps, Slate, Meagher & Flom LLP and its affiliates for educational and informational purposes only and is not intended and should not be construed as legal advice. This memorandum is considered advertising under applicable state laws.

One Manhattan West  
New York, NY 10001  
212.735.3000

## Revisions to the DOJ's Corporate Criminal Enforcement Policy Will Require Companies To Reevaluate Their Compliance Systems

In a recently published memorandum, Deputy Attorney General (DAG) Lisa Monaco announced important updates to the U.S. Department of Justice's (DOJ's) approach to investigating and prosecuting corporate crimes. In the document, DAG Monaco described these policy changes as a "combination of carrots and sticks" intended to empower corporate leaders to make a "business case for responsible corporate behavior."

The memo sets out higher expectations of corporations in a number of significant areas, ranging from compensation incentive systems to the use of third-party apps for company communications and the disclosure of misconduct when it is discovered — changes that will require companies to reexamine their compliance programs.

Prosecutorial uniformity and transparency are key themes throughout the memo, with DAG Monaco directing all DOJ components to adopt clear policies on certain issues, including a written policy to incentivize voluntary self-disclosure by companies. The memo also promises that further guidance will follow from other parts of the department.

The memo restores the DOJ's prior policy on individual misconduct, outlined in 2015 by Deputy Attorney General Sally Yates, which requires companies to disclose all nonprivileged information related to *all* individuals involved in corporate misconduct in order to receive cooperation credit. This policy was relaxed during the Trump administration to require disclosure only for individuals *substantially* involved in such misconduct.

DAG Monaco's memo also clarifies how the DOJ intends to weigh types of past misconduct in determining an appropriate resolution, including several specific directions to prosecutors that will help create a more uniform approach to treating a corporation's historic misconduct — including the prior misconduct of acquired entities.

Companies should take immediate steps to align compliance efforts with the new enforcement priorities and policies. Furthermore, in the event that a company becomes aware of misconduct or potential criminal activity, its response should be calibrated against the requirements of the memo to put itself in the best position to avoid a guilty plea or the imposition of an independent monitor.

# Revisions to the DOJ's Corporate Criminal Enforcement Policy Will Require Companies To Reevaluate Their Compliance Systems

---

## What steps can companies take now in response to the Monaco Memo?

Over the last year, DAG Monaco has been positioning DOJ to take a more aggressive and coordinated approach to investigating and prosecuting corporate crime. Based on the memo, here are key areas where companies should devote attention in evaluating their compliance systems:

### Compensation Programs

The memo sets forth, for the first time, a DOJ-wide policy regarding corporate compensation structures. Going forward, compensation structures will be a key metric used by prosecutors in evaluating a company's compliance program. Specifically, companies should take a close look at existing compensation systems and explore ways they can be modified to encourage compliance and discourage misconduct. Changes could include:

**Clawback Provisions.** Compensation structures that allow for retroactive discipline (*e.g.*, clawback provisions, escrowing of compensation) will be looked on especially favorably by the DOJ, since misconduct is often discovered after compensation has been paid. The memo seeks to usher in a new era where such arrangements are ubiquitous and routinely enforced to curb corporate crime. DAG Monaco has directed the Criminal Division to develop further guidance by the end of the year on how to reward corporations that develop and apply compensation clawback policies.

But putting these mechanisms into place will present a whole host of issues. For instance, what is the appropriate trigger for a clawback? An accusation? An adverse HR action? An indictment? A guilty plea or verdict?

In addition to issues surrounding the conditions for a clawback, the DOJ's expectation that companies will enforce these agreements poses additional challenges. Taking any action to dock pay opens the door to potential lawsuits alleging that compensation was improperly withheld or clawed back. Moreover, enforcement of these provisions and managing associated litigation risk may prove especially difficult in cross-jurisdictional cases and for multinationals with employees in jurisdictions with labor-friendly laws. Companies should carefully consider these issues as they begin to rethink compensation structures in light of the memo.

**Nondisclosure Agreements.** The use of nondisclosure agreements (NDAs) and nondisparagement provisions in compensation agreements should also be revisited in light of the memo, which suggests that negative inferences will be drawn to the extent these provisions inhibit the disclosure of misconduct.

Many NDAs already have whistleblower exceptions and carve-outs for reporting criminal activity. Companies should ensure that their agreements clearly articulate these exceptions to avoid any allegation that an employee was restricted by the agreement in reporting misconduct.

### Personal Devices and Third-Party Applications

Companies should also create or strengthen policies regarding the use of personal devices and third-party messaging platforms. The memo describes how the prevalence of personal devices and third-party messaging apps, which often allow for disappearing or encrypted messages, can present barriers to DOJ investigations, and it directs companies to implement policies to ensure that business-related data and communications are preserved and able to be produced to the government.

The memo does not propose a ban on disappearing chats and encrypted messaging apps. But DAG Monaco directed the Criminal Division to further study best corporate practices regarding third-party messaging platforms and provide additional direction to prosecutors.

Companies can begin positioning themselves now to be able to react quickly when that supplemental guidance comes down. For instance, they can create or strengthen policies governing personal devices and third-party messaging apps — and regularly train employees about these policies and enforce them. Companies should also take steps now to better understand how third-party messaging apps are used by executives and employees.

### Being the First To Know

The memo makes clear that a company will only receive cooperation credit for self-disclosure if the disclosure is made prior to an imminent threat of disclosure or government investigation. Companies should therefore ensure that their compliance programs incentivize employees to surface problems to management before the conduct becomes known to the government, and carefully review whether current reporting mechanisms (*e.g.*, whistleblower programs, compliance hotlines) are effectively alerting the company to problems.

### Overseas Investigations

Companies should also begin thinking through how to timely disclose issues arising from their non-U.S. operations, particularly where the underlying documentation may be protected by foreign blocking statutes, data privacy laws or other restrictions.

# Revisions to the DOJ's Corporate Criminal Enforcement Policy Will Require Companies To Reevaluate Their Compliance Systems

The memo directs prosecutors to provide credit to corporations that find ways to navigate these issues of foreign law and produce such records, but also imposes an adverse inference “where a corporation actively seeks to capitalize on data privacy laws and similar statutes to shield misconduct inappropriately from detection and investigation by U.S. law enforcement.”

The memo further establishes that the cooperating corporation in any DOJ investigation bears the burden of establishing the existence of foreign restrictions and identifying reasonable alternatives to provide the requested facts and evidence expeditiously — a rule that previously only applied in investigations under the Foreign Corrupt Practices Act.

Companies should continue to assess their obligations under foreign data privacy laws, including the penalties associated with potential violations (*i.e.*, whether the foreign law imposes criminal, civil or administrative penalties), and ensure that the positions it takes with respect to such laws are reasonable and consistent.

## **What should companies do if serious misconduct or criminal activity is discovered?**

Companies that become aware of serious misconduct or a potential criminal violation will be held to a high standard of cooperation under the memo. The benefit offered in exchange for such cooperation is significant: Absent aggravating factors, the “Department will not seek a guilty plea where a corporation has voluntarily self-disclosed, fully cooperated, and timely and appropriately remediated the criminal conduct.” Further, prosecutors will generally not impose an independent compliance monitor for a cooperating corporation that voluntarily self-discloses the relevant conduct if, at the time of resolution, the company also demonstrates that it has implemented and tested an effective compliance program.

The expectations for voluntary self-disclosure will continue to be clarified as DOJ components adopt further written policies, as directed by the memo. But one thing is certain: The DOJ wants

disclosure to happen *fast*, and it expects document preservation and production to quickly follow on a rolling basis. As Principal Associate Deputy Attorney General Marshall Miller stated in a [speech following publication of the memo](#), “[W]hen misconduct happens and the compliance program discovers it, we say: Pick up the phone and call us. Do not wait for us to call you.”

The demands of the policies articulated in the memo will undoubtedly be at odds with legitimate goals of the company at times. Even a thorough review of an issue by external counsel to determine the extent of the misconduct and early advocacy could take time that the company might not be allowed under the memo.

Near real-time reporting obligations also raise the question of what a company should do if it discovers misconduct that violates a company policy but is not strictly illegal, or if the misconduct falls in a gray area of the law. Furthermore, investigations involve many stakeholders, and the timeline for reporting obligations envisioned by the memo will pose challenges where reports must be made simultaneously to senior management and the company's board of directors, and buy-in must be obtained from them.

Companies should therefore think through an investigation strategically as soon as possible after discovering an issue, with a focus on the parameters outlined by the memo.

\* \* \*

DAG Monaco's memo is a helpful window into the DOJ's evolving compliance expectations of corporations and the factors the DOJ will consider in corporate criminal enforcement actions. Exactly how the DOJ will apply these standards, especially the newly minted policies, remains to be seen. The policies will be clarified as the written guidance mandated by DAG Monaco are issued. In the meantime, companies can begin taking steps to assess their compliance programs to better position themselves before the DOJ.

# Revisions to the DOJ's Corporate Criminal Enforcement Policy Will Require Companies To Reevaluate Their Compliance Systems

---

## Contacts

**Maria Cruz Melendez**

Partner / New York  
212.735.2320  
maria.cruzmelendez@skadden.com

**Gary DiBianco**

Partner / Washington, D.C.  
202.371.7858  
gary.dibianco@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

**Patrick Fitzgerald**

Partner / Chicago  
312.407.0508  
patrick.fitzgerald@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

**Bradley A. Klein**

Partner / Washington, D.C.  
202.371.7320  
bradley.klein@skadden.com

**Steve Kwok**

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

**David B. Leland**

Partner / Washington, D.C.  
202.371.7713  
david.leland@skadden.com

**Jessie K. Liu**

Partner / Washington, D.C.  
202.371.7340  
jessie.liu@skadden.com

**David Meister**

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

**William Ridgway**

Partner / Chicago  
312.407.0449  
william.ridgway@skadden.com

**Matthew E. Sloan**

Partner / Los Angeles  
213.687.5276  
matthew.sloan@skadden.com

**Chuck Smith**

Partner / Chicago  
312.407.0516  
charles.smith@skadden.com

**Lawrence S. Spiegel**

Partner / New York  
212.735.4155  
lawrence.spiegel@skadden.com

**Amy Van Gelder**

Partner / Chicago  
312.407.0903  
amy.vangelder@skadden.com

**Gretchen M. Wolf**

Partner / Chicago  
312.407.0956  
gretchen.wolf@skadden.com

**Khalil N. Maalouf**

Counsel / Washington, D.C.  
202.371.7711  
khalil.maalouf@skadden.com

**Michael A. Darling**

Associate / Washington, D.C.  
202.371.7563  
michael.darling@skadden.com