

Department of Justice Announces First-Ever Pilot Program on Compensation Incentives and Clawbacks, Revisions to Corporate Guidance Regarding Electronic Communications, and Resource Commitments for Corporate Compliance with Sanctions and Export Control Laws

by Nicole Engisch, John Marti, and Elena Modl

On March 2, 2023, in remarks delivered at the American Bar Association's National Institute on White Collar Crime, Deputy Attorney General Lisa Monaco announced a new policy creating incentives for companies to adopt compensation programs that emphasize compliance. She also unveiled new resource commitments to address the intersection between corporate crime and national security.

On March 3, 2023, Assistant Attorney General Kenneth Polite Jr. announced substantial revisions to the Department of Justice's (DOJ) corporate compliance guidance, including provisions governing preservation of electronic business-related communications, communications through third-party applications, and the use of personal devices.

Pilot Program on Compensation Incentives and Clawbacks

The Pilot Program is a three-year initiative addressing compensation policies, including the "clawing back" of compensation from employees who engage in misconduct. The guidance aims to reward corporate compliance with tangible financial incentives: companies will receive reduced fines if they attempt to claw back compensation paid out to corporate wrongdoers. The two-part program consists of the following:

- 1. Corporate resolutions will now require the involved company to develop compliance-promoting criteria within its compensation and bonus structures.**

Resolving companies must structure compensation and bonus systems around compliance and provide annual implementation reports to the DOJ, Criminal Division. Standards could include, but are not limited to:

Related People

- Nicole Engisch
- John Marti
- Elena Modl

Related Capabilities

- Corporate Governance & Compliance
- Executive Compensation
- Government Enforcement & Corporate Investigations
- National Security Law
- Technology

1. Prohibiting bonuses for employees failing to satisfy compliance requirements;
2. Penalizing employees engaging in misconduct and those who (a) maintained supervisory authority over the employees or business area engaging in wrongful conduct and (b) had knowledge of or demonstrated willful blindness to the misconduct; and
3. Incentivizing those who fully commit to compliance procedures.

Practice Point: Companies should work with counsel and compliance officers to consider appropriate changes to compensation policies incentivizing compliance. These could include adding compliance-related metrics to compensation formulas or performance reviews, such as the forfeiture of bonuses and other compensation for failure to follow compliance procedures or for allowing supervisees to engage in misconduct. The DOJ recommends defining clear and effective financial penalties to deter misconduct and risky behavior. Companies should consult counsel experienced in corporate compliance and complicated employment matters to discuss the pros and cons of adopting compensation policy changes to conform to the DOJ policy guidance.

2. Companies that *attempt* to claw back compensation from individuals engaging in misconduct will receive a credit against fines.

At the outset of a resolution with the government, the involved company will pay the applicable penalty in full, but will receive a credit equal to the amount it will attempt to claw back from individual wrongdoers (Possible Clawback Reduction). Prosecutors will then reduce the fine by 100% of the compensation recovered during the period of resolution.

1. **If the company recoups full compensation** from the employees responsible for the misconduct by the end of the resolution term, it will keep the clawed back funds.
2. **If the company recoups partial payment** of the amount it sought to claw back, it will be required to pay back the difference between the Possible Clawback Reduction and the funds actually recovered.
3. **Importantly, companies who attempt to claw back compensation in good faith, but without success, will still be eligible for a fine reduction of up to 25% of the amount sought in the attempted clawback.**

Such discretionary fine reductions may be justified where a company incurred significant legal costs in its attempt to claw back the funds or if the company can demonstrate a likelihood of recouping the compensation after the resolution period ends. The applicable fine reduction will not affect funds recovered via restitution, disgorgement, or other form of agreed-upon payment.

Practice Point: DAG Monaco recognized that the pursuit of clawbacks is expensive and difficult. Moreover, the effort may be unsuccessful to the extent a clawback may conflict with employment laws or employment contracts. The pilot program accounts for these challenges by rewarding companies that are willing to make the effort. Companies should consult with outside counsel to evaluate the effectiveness of compliance programs and to consider needed modifications to compliance programs, potentially to

include clawback and other changes to compensation policies. To maximize the potential for declinations and fine reductions and to prevent or minimize wrongdoing in the first place, companies should improve their compliance program *before* they are faced with allegations of corporate wrongdoing.

The pilot program's goal is to shift the burden of corporate malfeasance away from uninvolved shareholders and onto those directly responsible for the misconduct. The DOJ hopes to empower companies, their counsel, and their compliance officers to push for investment in compliance by offering tangible incentives to present to their boardrooms.

Resource Commitments to Corporate Criminal Enforcement and National Security.

DAG Monaco also announced significant resource commitments to address the intersection of corporate crime and national security. The surge in resources includes the hiring of 25 new prosecutors in the National Security Division as well as the hiring of its first-ever Chief Counsel for Corporate Enforcement. The Division is increasing its capacity to prosecute corporate violations through new partnerships with the U.S. Attorneys' Offices and the Criminal Division. Similar to guidance issued by the Foreign Corrupt Practices Act (FCPA) and the Securities Exchange Commission (SEC), the National Security Division will issue joint advisories with the Commerce and Treasury Departments to inform the private sector about national security-related compliance and enforcement trends. DAG Monaco also announced an investment in the Bank Integrity Unit housed in the Money Laundering and Asset Recovery Section.

DAG Monaco concluded by emphasizing the DOJ's prioritization of holding individuals accountable for corporate malfeasance. The goal of these newly unveiled policies is to encourage companies to invest in robust compliance programs through incentives that are good for business.

Evaluation of Corporate Compliance Program Guidance – Messaging Applications

On March 3, 2023, Assistant Attorney General Kenneth Polite Jr. announced substantial revisions to the DOJ's compliance program guidance, focusing his remarks on corporate preservation of electronic communications, including those made on personal devices and through third-party applications. Particularly in the age of remote work, employees increasingly rely on personal devices and third-party messaging applications to conduct company business.

The DOJ will evaluate whether companies have effective electronic data governance policies as part of their compliance programs, the extent to which companies communicate such policies to employees, and whether companies follow through with enforcement. Prosecutors will specifically consider a corporation's policies regarding the use of personal devices and messaging applications. Companies should tailor policies to their specific risk profile and provide for access to and preservation of all business-related communications.

When conducting an evaluation of the corporate use of personal devices and communication platforms, the DOJ guidance instructs prosecutors to consider the following factors:

1. Electronic communication channels, preservation mechanisms, and retention policies.
2. “Bring Your Own Device” (BYOD) programs and accompanying preservation policies governing corporate data and communications.
3. Risk management and disciplinary measures for employees that refuse to give companies access to corporate data stored on personal devices.

AAG Polite emphasized that prosecutors will question companies that do not produce data from third-party communication applications, including ephemeral messaging applications. The expectation is that companies maintain access to these corporate communications and preserve them on corporate servers. AAG Polite stated that **a company’s lack of responsive answers will change any offer of criminal liability resolution**. Thus, business-related communications must be adequately monitored and preserved when necessary to avoid costly legal fines.

Practice Point: Companies should work with compliance officers as well as outside counsel to adopt appropriate policies governing electronic communications and other electronically stored information (ESI). In addition, companies should retain outside vendors skilled in collecting, managing, and reviewing electronic data to tailor solutions for the monitoring of applications used by employees for business-related communications. Dorsey’s LegalMine Document Review Solutions is skilled in providing such services.

In adopting appropriate policies to comply with the DOJ guidance, companies should consider:

1. Assessing the use of third-party messaging applications, particularly those supporting ephemeral messaging.
2. Outlining clear policies and holding employee trainings on appropriately using personal devices to conduct company business.
3. Valuing BYOD policies and the use of consent forms allowing company access to business-related communications on personal devices.
4. Evaluating preservation and retention policies of company data created on third-party applications and personal devices.

<https://www.justice.gov/opa/speech/file/1571906/download>

<https://www.justice.gov/opa/speech/file/1571911/download>