PAUL HASTINGS

Stay Current

October 2024

Follow @Paul_Hastings

DOJ Criminal Division Issues Updated Guidance on Corporate Compliance Programs Focused on AI Risks

By Nathaniel B. Edmonds, Leo Tsao, Nisa R. Gosselink-Ulep, Craig Y. Lee, Joanne Joseph, Margaret Shields & Noreen Mary Verini

I. INTRODUCTION

On September 23, 2024, the Department of Justice's ("DOJ") Criminal Division announced significant changes to its *Evaluation of Corporate Compliance Programs* ("ECCP"), which prosecutors use in assessing the effectiveness of corporate compliance programs. The changes to the ECCP cover a range of compliance topics, but most notably focus on steps companies should be considering to mitigate the increasing risks of artificial intelligence ("AI") and other new technologies. DOJ also discussed the application of earlier policies covering compensation incentives and whistleblower awards. These latest announcements continue DOJ's efforts to provide transparency and guidance for companies on how DOJ evaluates corporate compliance programs and how that can impact enforcement resolutions.

II. RECENT UPDATES TO THE EVALUATION OF CORPORATE COMPLIANCE PROGRAMS GUIDANCE

DOJ repeated its long-stated policy that its assessment of corporate compliance programs is "critical" to corporate resolutions because DOJ considers "not just what happened but why it happened and what the company has done to prevent misconduct from recurring." DOJ confirmed that just as companies are expected to continuously improve their compliance programs, DOJ regularly evaluates and updates its policies and enforcement tools, including the ECCP, "which is an invaluable resource to companies." The updated ECCP provides new guidance and clarity regarding AI and other new technology, "speak up" culture, data access, and other topics.

A. Artificial Intelligence and Other New Technology

Under the revised ECCP, prosecutors in the Criminal Division will evaluate how companies assess and manage risk related to the company's use of new technology, such as AI, both in their business and in their compliance programs. Prosecutors will consider the technology used, whether the company has conducted a risk assessment of the use of that technology, and whether the company has taken necessary steps to mitigate risks of that technology, including employee training, using human decision-making baselines, and protecting against intentional misuse of the technology. Prosecutors will also consider whether a company monitors and tests its technology to evaluate if it is working as intended and consistent with the company's code of conduct and enterprise risk management strategies.

Artificial intelligence continues to dominate the headlines and, as we have discussed previously, will be an important issue for DOJ to assess when companies are facing liability.

B. "Speak Up" Culture

Prosecutors in the Criminal Division will now specifically evaluate whether the company fosters a culture that encourages employees to speak up and report misconduct. Questions include whether individuals know how to report concerns and feel comfortable doing so, and whether the company encourages and incentivizes reporting of potential misconduct, or conversely, whether the company uses practices that tend to "chill" such reporting. Prosecutors will also consider the company's commitment to anti-retaliation policies and treatment of employees who report misconduct.

C. Data Resources and Access

Under the updated ECCP, prosecutors will assess whether compliance personnel have adequate access to data, assets, resources, and technology and will examine the resources that the company uses to leverage data for compliance purposes and compare that against those used for business purposes. Prosecutors will also consider how the company manages the quality of its data sources and measures the accuracy, precision, or recall of its data analytics models.

D. Other Notable Updates

1. **Applying Lessons Learned**. The ECCP now sets forth that a company should be using lessons learned from both its own prior misconduct and issues at other companies. Prosecutors will also consider whether a company's compliance program has a track record of preventing or detecting other instances of misconduct and if it exercised due diligence to prevent and detect misconduct.

2. **Identifying Emerging and Evolving Risks through Proactive Risk Management**. Risk assessments should account for emerging risks, such as AI, as the company's risk profile evolves. Prosecutors will now evaluate what features of the company reduce its exposure to risks and whether the company's approach to risk management is proactive or reactive.

3. **Additional Guidance on Mergers & Acquisitions**. Prosecutors will now consider whether a company's integration process accounts for migrating or combining critical enterprise resource planning ("ERP") systems and the extent to which compliance and risk management functions are involved in designing and executing the integration strategy. Prosecutors will also focus on the company's process for ensuring appropriate compliance oversight and risk assessment of the new business post-transaction.

4. **Continuous Improvement, Periodic Testing, and Review**. Prosecutors will now consider whether a company can demonstrate that it is proactively identifying misconduct or compliance issues at the earliest stage possible.

III. EFFECTIVENESS OF RECENT APPROACHES RELATING TO COMPENSATION INCENTIVES AND WHISTLEBLOWERS

DOJ also provided updates on two policies—the Compensation Incentives and Clawbacks Pilot Program and the Corporate Whistleblower Awards Pilot Program.

A. Compensation Incentives and Clawbacks Pilot Program

DOJ stated that it has so far required nine companies that have entered into corporate resolutions with the Criminal Division to embed compliance-related criteria into their compensation and bonus systems. For example, companies have incorporated compliance criteria in annual reviews and performance review metrics.

In addition, several companies have withheld compensation based on misconduct. This was an important aspect of remediation considered in two recent enforcement actions, where the companies received fine reductions of 40% and 45%, respectively. DOJ noted that withholding compensation from culpable employees sends "a clear message . . . that misconduct will have individual financial consequences."

B. Corporate Whistleblower Awards Pilot Program

DOJ also provided an update on its approach to corporate whistleblower awards, a critical tool to incentivize reporting of misconduct, which we wrote about in a previous client alert. Since its launch in August, DOJ's program on whistleblowers has already generated tips from over 100 whistleblowers. DOJ reiterated that it takes the risks whistleblowers face seriously and is committed to monitoring the actions that a company takes against whistleblowers. This commitment echoes DOJ's updates to the ECCP that reinforce the importance of "speak up" culture.

DOJ also emphasized that it recognizes when companies invest in implementing effective compliance programs, ensure compliance officers have a seat at the table, and move swiftly to cooperate and remediate when misconduct occurs. Companies that take these critical steps are in the best position to achieve the most favorable outcomes with the Criminal Division.

IV. KEY TAKEAWAYS FOR COMPANIES

DOJ continues to raise the bar for corporate compliance programs and the most recent ECCP update provides more specific guidance about several topics. While each topic is relevant to implementing an effective compliance program, companies should take particular note of DOJ's comments about AI, access to data, and "speak up" culture.

1. Companies should periodically evaluate their use of AI—and other new technology—for business and compliance activities to identify risks and implement mitigation strategies, including ongoing monitoring of reliability and how human judgment is used to assess appropriateness of AI-driven activities.

2. Companies should provide their compliance teams with systems, technology, and data, and consider whether it is reasonably proportionate to the resources used for supporting business operations.

3. To measure the effectiveness of "speak up" culture, companies can use employee surveys and analyze metrics from its reporting channels, which can be benchmarked against the metrics of other companies. For example, if a company's number of reports is much lower or its rate of anonymous reporting is much higher compared to a similarly situated company that could be a sign that employees do not feel comfortable reporting their concerns and potentially fear retaliation.

4. Companies should take note of DOJ's rising expectations for compliance programs and its more detailed feedback on evaluating specific aspects of a corporate compliance program, including how the company:

   a. Protects employees from retaliation through following up periodically with concern raisers or tracking employment actions;

   b. Evaluates whether employees actually understand and learn from trainings through knowledge checks, follow-up surveys, or other assessment mechanisms;

   c. Accounts for an acquired company's ERP systems as part of its post-acquisition integration; and

   d. Compiles risks identified from multiple internal and external sources, such as risk assessments, investigations, ongoing monitoring activities, and issues experienced by other companies, and continuously enhances its compliance program to address these risks, including through revised policies, updated trainings, targeted communications, or other system or process changes.

5. Although these policies are limited to the prosecutors of the Criminal Division, from an antitrust perspective, companies should address key risk areas including cartels and other anticompetitive conduct. For example, the Antitrust Division has also expressed increased interest in working with members of the business community to protect whistleblowers. The Antitrust Division has taken steps to promote access through the Antitrust Division's website and Citizen Complaint Center so that members of the public can register antitrust complaints and concerns more efficiently. Companies should consider and monitor developments relating to the interplay between potential increased cartel whistleblowers and the Antitrust Division's Leniency Policy.

✧ ✧ ✧

If you have any questions concerning these developing issues, please do not hesitate to contact any of the following Paul Hastings lawyers:

Washington D.C.

Nathaniel B. Edmonds
1.202.551.1774
nathanieledmonds@paulhastings.com

Nisa R. Gosselink-Ulep
1.202.551.1746
nisagosselinkulep@paulhastings.com

Craig Y. Lee
1.202.551.1752
craiglee@paulhastings.com

Leo Tsao
1.202.551.1910
leotsao@paulhastings.com

Joanne Joseph
1.202.551.1909
joannejoseph@paulhastings.com