

Antitrust Division's Updated Guidance on Evaluating Corporate Compliance Programs — Key Features and Takeaways

The guidance stresses heightened focus on emerging antitrust risks, enhanced support and incentives, and proactive monitoring.

On November 12, 2024, the Antitrust Division of the US Department of Justice (the Antitrust Division) released updated guidance for its prosecutors on evaluating corporate compliance programs (the Guidance).¹ The Guidance supersedes the Antitrust Division's original 2019 compliance guidance² by again tracking similar updated guidance that the Department of Justice's (DOJ) Criminal Division issued in September 2024.³

However, the Guidance includes several unique additions that provide more insight into how Antitrust Division prosecutors will assess the effectiveness of corporate compliance programs in the context of criminal violations of the Sherman Act for price fixing, bid rigging, market allocation, and monopolization, as well as acts of obstruction that imperil antitrust investigations.⁴ The Antitrust Division also announced that companies seeking to resolve *civil* antitrust violations should expect the Guidance to be used when they ask the Antitrust Division to credit a compliance program to achieve a more favorable disposition in a civil context.

The Antitrust Division reviews corporate compliance programs when they are (1) making charging decisions and (2) making sentencing recommendations (that could include reporting or independent compliance monitor obligations). It will assess the program in place at the time of the offense, and subsequent improvements after the offense. The Antitrust Division makes clear in the Guidance that it will not just accept a company's representations and instead instructs prosecutors to conduct their own investigation, including asking compliance-related questions of witnesses. This proactive approach to evaluating the efficacy of compliance programs appears to be part of a DOJ-wide push, and companies should expect compliance-related inquiries to feature in investigations, even at early stages.

The Antitrust Division notes that it will take into account the size and resources of the organization such that large organizations are expected to devote more formal operations and more resources than smaller organizations. However, the Guidance conveys that high standards will apply to all.

Antitrust Division's Historical Approach to Compliance Programs

In 2019, the Antitrust Division announced for the first time that it would consider offering credit to corporations involved in criminal antitrust investigations for robust pre-existing compliance programs as part of charging decisions and making sentencing recommendations.⁵ Prior to 2019, the Antitrust Division had a “winner-take-all” treatment of cartel participants who were first to report under the Corporate Leniency Policy by refusing to offer any credit at the charging or sentencing phase for a compliance program.⁶

The Antitrust Division maintains that an “effective” compliance program “should prevent many of the most egregious violations...and the program should enable a company to swiftly, detect, and address them, including giving the company the best chance to self-report and qualify for the Antitrust Division's Leniency Program.”⁷ This leaves open the possibility that the Antitrust Division could find that a compliance program satisfied the elements in the Guidance, even if a violation occurred that was not timely detected and reported as part of a leniency application. Nonetheless, the bar still remains high for the Antitrust Division to find a compliance program to have been “effective” in the face of a violation.

Elements of Effective Compliance Programs: The Antitrust Division's View

While the Antitrust Division refers to the same elements as the Criminal Division in evaluating the effectiveness of a compliance program, its Guidance also provides more specific insight into the factors Antitrust Division prosecutors should consider in determining whether the elements were satisfied.

1. ***Design and Comprehensiveness:*** In line with Criminal Division guidance, compliance programs should be integrated into business practices and be easily accessible to employees. Programs must be regularly updated to address emerging risks and technological developments. The Guidance also newly cautions prosecutors to keep in mind that programs may “reflect efforts to meet standards across a number of areas of law and jurisdictions,”⁸ a potentially helpful recognition for companies with global compliance programs in which certain compliance mechanisms may not be permissible in some jurisdictions (e.g., according to data privacy and employment law).

The Antitrust Division places additional emphasis on the following specific overarching requirements:

- **Adequate emphasis on antitrust compliance:** The Guidance places new focus on whether antitrust compliance is “given appropriate emphasis in light of the antitrust risks the company faces” within a larger compliance program. This requirement puts the responsibility on the company to assess its risk profile and then build a program tailored to that risk profile so that businesses with elevated antitrust risk will be expected to prioritize antitrust compliance in particular.

The Guidance also borrows from the updated Criminal Division guidance to add inquiries on whether “there were requests for resources from the compliance function that were denied” and specifically asks for a comparison of the resources allocated to antitrust compliance compared to other company functions as well as “the level of technology devoted to compliance comparable to the level of technology devoted to other functions.”⁹

- **Updating programs to cover expanding antitrust non-compliance risk:** The Guidance asks, “[a]re the compliance program and compliance materials updated to account for newly developed technology and emerging risks?”¹⁰ Throughout it refers to artificial intelligence-related risks, earmarking them for special attention.

- **Accountability for various modes of communication:** The Guidance stresses the need for clear guidelines on means of communication and comprehensive document retention policies that account for ephemeral messaging and non-company methods of communication. This is part of a DOJ-wide emphasis on managing and preserving electronic communications that puts companies on notice that non-compliance could be dealt with harshly.¹¹
2. *Culture of Compliance:* The Antitrust Division joins the Criminal Division in emphasizing the importance of leaders and managers actively fostering a culture of compliance throughout all levels of the organization but also stresses the expectation for an antitrust-specific focus.¹²

The Guidance emphasizes that the Antitrust Division will scrutinize whether antitrust violations have been tolerated in the pursuit of “new business, greater revenues, hiring or retaining employees, market share, or maintaining customers, territories, or markets,”¹³ and also whether hiring and compensation reinforces an ethical and compliant culture and how that has been measured. The Guidance signals a focus on the board of directors and external auditors and whether they have expertise and exposure to the antitrust compliance and control functions.

3. *Responsibility for the Program:* The Guidance refers to not only the need for adequate resources, but also the need to have “qualified personnel” with experience dedicated to compliance who have tenure in their position (“without excessive turnover”) and report to senior leaders and the board of directors.¹⁴ Companies with an elevated risk profile should engage personnel familiar with antitrust law and who are able to recognize potential antitrust violations in connection with their compliance programs.
4. *Risk Assessment:* Compliance programs should be specifically tailored to address a company’s unique antitrust risks, considering its line of business and technological use, and should be regularly updated and reviewed. For the first time, the Guidance adds an inquiry into whether the company conducted a gap analysis to identify where risks are not sufficiently covered and then prioritize higher-risk areas to ensure resources are effectively allocated.
 - **Technology risks:** The Antitrust Division joins the Criminal Division in emphasizing the recognition and management of risks associated with technology, including artificial intelligence (AI)¹⁵ and specifically adds a reference to “algorithmic revenue management.”¹⁶ This focus correlates to an enforcement push by the Antitrust Division to prosecute price fixing and unlawful information exchanges involving pricing algorithms.¹⁷ It asks whether personnel involved in the deployment of AI are able to assess risks posed and whether compliance personnel are able to detect and correct decisions made by AI when they are “not consistent with the company’s values.”¹⁸ Companies should be aware of this expectation that they are actively managing these risks.
5. *Training and Communication:* Employees should be well-informed about their compliance obligations, with antitrust policies clearly included in the company’s code of conduct. The Guidance emphasizes addressing any barriers to implementing these policies, particularly in foreign subsidiaries. It also directs prosecutors to ask whether the employees know how to access compliance materials, how to engage with them, and whether the focus of training is on compliance or detection avoidance. In line with the added emphasis on technology risks, the Guidance also inquires whether training “address[es] permissible and nonpermissible uses of new technology including AI.”¹⁹

The Guidance further emphasizes the following expectations:

- **Targeted training of certain “high risk” groups of employees:** Companies should train employees who have authority over pricing or market strategy, participate in industry meetings, or are involved in bidding certifications or human resources decisions.
 - **Training on lessons learned and with the benefit of business knowledge:** Companies should make training more relevant by tailoring materials to the industries in which the company operates or specific antitrust violations that have occurred in those industries in the past. They should consult with business units before implementing policy changes to ensure that updates are informed by practical insights and operational realities.
 - **Timely, regular, and accessible training:** Companies should inform individuals of risky activities in advance, such as during employee onboarding or before attending trade shows and trade association meetings, and should make sure that the compliance guidance can be easily assessed and that individuals are regularly trained.
 - **Testing understanding of the risks:** Companies should ensure that relevant personnel understand the risks, making particular note that compliance personnel and managers should be trained to identify antitrust “red flags.” Training should take into account emerging risks, particularly when communicating and collaborating with competitors, including both within and outside of legitimate joint ventures, often through testing and certifications.
 - **Emphasis on compliance rather than avoiding detection:** Companies should ensure the understanding of antitrust laws, and, importantly, if personnel are educated on the use of antitrust “hot” words, the emphasis should be on detecting or deterring violations rather than avoiding detection by enforcers.
6. *Monitoring and Auditing:* The Guidance cautions that companies should regularly update their risk assessments and for the first time urges an inquiry into whether gap analyses were conducted to identify and address potential weaknesses and amend the program to account for previous violations in the company and industry.
- The Antitrust Division directs prosecutors to further evaluate whether companies use screening tools, communications monitoring, or other testing methods to identify potential violations. The Guidance instructs prosecutors to probe into how company data is used to audit and monitor employees and whether compliance personnel can assess such data promptly. The Guidance further inquires into the process for reviewing “monitored communications” of employees and the actions taken as a result of identified issues.²⁰
 - For the first time, the Guidance also notes that prosecutors will consider monitoring AI-made decisions, such as pricing recommendations, to ensure compliance with antitrust laws.
 - The Guidance speaks to an expectation that the company will deploy internal controls to monitor higher-risk activities, such as by tracking competitor interactions with attendance at trade association meetings, trade shows, and other industry gatherings.
7. *Reporting Mechanisms:* Compliance systems should facilitate confidential reporting of potential violations without fear of retaliation. In line with Criminal Division guidance, the Antitrust Division underscores the importance of a trusted process that includes protections for whistleblowers and ensures thorough investigations of reported concerns. In particular, the Antitrust Division stresses its expectation that companies use non-disclosure agreements (NDAs) and have other employee

policies that make clear that employees can report antitrust violations internally and to government authorities and that they are entitled to protection under Criminal Antitrust Anti-Retaliation Act (CAARA). Specifically, the Guidance instruct prosecutors to:

- add inquiries as to how a company “determine[s] which antitrust complaints and red flags merit further investigation[,]”²¹ and how it ensures that the investigations are “independent, objective, appropriately conducted, and properly documented”;²²
- emphasize the importance of training employees on the protections provided under the CAARA; and
- examine whether the use of NDAs deters whistleblowers or violates CAARA.²³

8. *Incentives and Discipline:* Compliance systems should be designed to promote compliance and effectively address violations. The Guidance evaluates whether incentives, compensation structures, or rewards are in place for adhering to the compliance policy, as well as any actions taken in response to compliance violations, such as denied promotions or clawed-back bonuses.

9. *Remediation Methods and Role of Program:* The Guidance then notes that compliance programs should be evaluated based on whether they incorporate the following:

- **Early Detection and Self-Policing:** The Antitrust Division emphasizes the importance of early detection and self-policing, which can enhance a company’s eligibility for Type A of the Corporate Leniency Policy.²⁴ “If a compliance program did effectively identify misconduct, including allowing for timely remediation and self-reporting (but not in time to qualify for leniency), a prosecutor should view the occurrence as a strong indicator that the compliance program was working effectively,” and therefore is also relevant at the charging stage of an investigation.²⁵
- **Root Cause Analysis:** For the first time, prosecutors are instructed to assess a company’s analysis of the root cause of the antitrust misconduct, the compliance program’s role in uncovering the violation, the role of managers and leaders, the systematic issues that arose, and which controls failed.
- **Remedial Actions:** In the event of a violation, prosecutors will evaluate whether a company has taken appropriate remedial actions, such as revising the compliance program in response to the incident. Prosecutors are instructed to inquire about senior leadership’s role in the violation and, for the first time, to evaluate whether those involved were disciplined.

If you have questions about this Client Alert, please contact one of the authors listed below or the Latham lawyer with whom you normally consult:

Elizabeth Prewitt

elizabeth.prewitt@lw.com
+1.212.906.1354
New York / Washington, D.C.

Samantha Sosa

samantha.sosa@lw.com
+1.212.906.4633
New York

Ashley M. Bauer

ashley.bauer@lw.com
+1.415.395.8138
San Francisco

Belinda S Lee

belinda.lee@lw.com
+1.415.395.8851
San Francisco

Niall E. Lynch

niall.lynch@lw.com
+1.415.395.8162
San Francisco

You Might Also Be Interested In

[Webcast: A Look Ahead: The Trump Administration's Regulatory and Enforcement Priorities](#)

[FTC Adopts Major Changes to HSR Merger Notification Form](#)

[10 Key Takeaways — Developments in International Cartel Enforcement and Observations From the International Cartel Workshop](#)

Client Alert is published by Latham & Watkins as a news reporting service to clients and other friends. The information contained in this publication should not be construed as legal advice. Should further analysis or explanation of the subject matter be required, please contact the lawyer with whom you normally consult. The invitation to contact is not a solicitation for legal work under the laws of any jurisdiction in which Latham lawyers are not authorized to practice. A complete list of Latham's Client Alerts can be found at www.lw.com. If you wish to update your contact details or customize the information you receive from Latham, [visit our subscriber page](#).

Endnotes

¹ See [U.S. DOJ Antitrust Division November 2024 Evaluation of Corporate Compliance Programs](#).

² See <https://www.justice.gov/opa/pr/antitrust-division-announces-new-policy-incentivize-corporate-compliance>

³ See <https://www.justice.gov/criminal/criminal-fraud/page/file/937501/dl>

⁴ 15 U.S.C. § 1

⁵ The DOJ will evaluate the effectiveness of a company's antitrust compliance program when making sentencing reduction recommendations. See U.S. DOJ Antitrust Division, Evaluation of Corporate Compliance Programs in Criminal Antitrust Investigations, at 17–19 (Nov. 2024), <https://www.justice.gov/atr/media/1376686/dl?inline=#:~:text=The%20guidance%20aids%20Antitrust%20Division,or%20an%20independent%20compliance%20monitor>

⁶ See New DOJ Guidance Increases Benefits for Robust Antitrust Compliance Programs — What Companies Need to Know, Latham & Watkins, at 1 (July 16, 2016), <https://www.lw.com/admin/upload/SiteAttachments/Alert%202525.v2.pdf>

⁷ See U.S. DOJ Antitrust Division, Evaluation of Corporate Compliance Programs in Criminal Antitrust Investigations, at 2 (Nov. 2024), <https://www.justice.gov/atr/media/1376686/dl?inline=#:~:text=The%20guidance%20aids%20Antitrust%20Division,or%20an%20independent%20compliance%20monitor>

-
- ⁸ See U.S. DOJ Antitrust Division, Evaluation of Corporate Compliance Programs in Criminal Antitrust Investigations, at 4 (Nov. 2024), <https://www.justice.gov/atr/media/1376686/dl?inline=#:~:text=The%20guidance%20aids%20Antitrust%20Division,or%20an%20independent%20compliance%20monitor>
- ⁹ *Id.* at 8.
- ¹⁰ *Id.* at 5.
- ¹¹ See Deputy Attorney General Luis Monaco, Further Revisions to Corporate Criminal Enforcement Policies Following Discussions with Corporate Crime Advisory, at 11 (Sep. 15, 2022), <https://www.justice.gov/media/1245451/dl>. Also see U.S. Department of Justice, Justice Department and the FTC Update Guidance that Reinforces Parties' Preservation Obligations for Collaboration Tools and Ephemeral Messaging (Jan. 26, 2024), <https://www.justice.gov/opa/pr/justice-department-and-ftc-update-guidance-reinforces-parties-preservation-obligations>
- ¹² "Prosecutors should examine the extent to which corporate management—both senior leadership and managers at all levels—has clearly articulated and conducted themselves in accordance with the company's commitment to good corporate citizenship." See Evaluation of Corporate Compliance Programs, at 6, [U.S. DOJ Antitrust Division November 2024 Evaluation of Corporate Compliance Programs](https://www.justice.gov/atr/media/1376686/dl?inline=#:~:text=The%20guidance%20aids%20Antitrust%20Division,or%20an%20independent%20compliance%20monitor).
- ¹³ See U.S. DOJ Antitrust Division, Evaluation of Corporate Compliance Programs in Criminal Antitrust Investigations, at 7 (Nov. 2024), <https://www.justice.gov/atr/media/1376686/dl?inline=#:~:text=The%20guidance%20aids%20Antitrust%20Division,or%20an%20independent%20compliance%20monitor>
- ¹⁴ The Antitrust Division evaluates several factors, including: who is responsible for the antitrust compliance program and their reporting structure; how the compliance function compares to other company areas in terms of experience, rank, resources, and access to key leaders; whether personnel are fully dedicated to compliance responsibilities, and if not, the proportion of their time allocated to these duties; whether the company provides sufficient resources for employee training; whether requests for resources are fulfilled or denied; and who reviews the effectiveness of the compliance function and the nature of the review process. *Id.* at 7-8.
- ¹⁵ Notably, AI is defined broadly so that "no system should be considered too simple to qualify as a covered AI system due to lack of technical complexity."
- ¹⁶ See U.S. DOJ Antitrust Division, Evaluation of Corporate Compliance Programs in Criminal Antitrust Investigations, at 9 (Nov. 2024), <https://www.justice.gov/atr/media/1376686/dl?inline=#:~:text=The%20guidance%20aids%20Antitrust%20Division,or%20an%20independent%20compliance%20monitor>
- ¹⁷ See, e.g., U.S. Department of Justice, Justice Department Sues RealPage for Algorithmic Pricing Scheme that Harms Millions of American Renters (Aug. 23, 2024), <https://www.justice.gov/opa/pr/justice-department-sues-realpage-algorithmic-pricing-scheme-harms-millions-american-renters>
- ¹⁸ See U.S. DOJ Antitrust Division, Evaluation of Corporate Compliance Programs in Criminal Antitrust Investigations, at 10 (Nov. 2024), <https://www.justice.gov/atr/media/1376686/dl?inline=#:~:text=The%20guidance%20aids%20Antitrust%20Division,or%20an%20independent%20compliance%20monitor>
- ¹⁹ See U.S. DOJ Antitrust Division, Evaluation of Corporate Compliance Programs in Criminal Antitrust Investigations, at 12 (Nov. 2024), <https://www.justice.gov/atr/media/1376686/dl?inline=#:~:text=The%20guidance%20aids%20Antitrust%20Division,or%20an%20independent%20compliance%20monitor>
- ²⁰ *Id.* at 13.
- ²¹ See U.S. DOJ Antitrust Division, Evaluation of Corporate Compliance Programs in Criminal Antitrust Investigations, at 14 (Nov. 2024), <https://www.justice.gov/atr/media/1376686/dl?inline=#:~:text=The%20guidance%20aids%20Antitrust%20Division,or%20an%20independent%20compliance%20monitor>
- ²² *Id.*
- ²³ 15 U.S.C. § 7a-3
- ²⁴ "Type A is available before the Division has opened an investigation, provided the Division has not received information about the illegal activity from any other source and the other criteria for Type A Leniency are met." FREQUENTLY ASKED QUESTIONS ABOUT THE ANTITRUST DIVISION'S LENIENCY PROGRAM, U.S. Department of Justice, at 7 (January 3, 2023), <https://www.justice.gov/atr/page/file/1490311/dl>
- ²⁵ See U.S. DOJ Antitrust Division, Evaluation of Corporate Compliance Programs in Criminal Antitrust Investigations, at 15–16 (Nov. 2024), <https://www.justice.gov/atr/media/1376686/dl?inline=#:~:text=The%20guidance%20aids%20Antitrust%20Division,or%20an%20independent%20compliance%20monitor>