VENABLE LLP

DOJ Revises Its Evaluation of Corporate Compliance Policy to Consider How Companies Address Risks Posed by AI

Is Your Corporate Culture of Compliance Keeping up with Emerging Technology Trends

October 08, 2024

Kan M. Nawaday, Adrienne Dawn Gurley, Steven E. Swaney and Lauren M. Modelski

The Department of Justice's Criminal Division is "using more tools than ever before to identify corporate misconduct and to encourage companies to be good corporate citizens," according to Nicole Argentieri, Principal Deputy Attorney General and head of DOJ's Criminal Division. This new tool kit already includes a recently launched whistleblower reward program, which, only two months after its formal launch, has fielded over 100 new tips.

DOJ's tool kit has now been enhanced to include new guidance for prosecutors in the form of recent updates to assess the effectiveness of corporate compliance programs. Specifically, Argentieri announced changes to the Criminal Division's Evaluation of Corporate Compliance Programs policy ("ECCP"), which provides guidance to prosecutors to make informed decisions about whether "and to what extent" a company's "compliance program was effective at the time of [an] offense, and is effective at the time of a charging decision or resolution...." These changes direct prosecutors to look at how corporations safeguard against the risks of emerging technologies, such as AI, and how corporations are using AI and other resources to bolster their compliance programs.

Ensuring Safeguards Against Technology-Related Risks

The new amendments to the ECCP provide that prosecutors should consider, among other things:

- Whether a company has a process to identify and manage emerging internal and external risks that "could potentially impact the company's ability to comply with the law, including risk related to the use of new technologies"
- How a company assesses the impact of new technologies, such as AI, on its ability to comply with criminal laws
- Whether a company's management of risk associated with the use of AI is integrated into "broader enterprise risk management (ERM) strategies"
- A company's approach to governance regarding the use of new technologies, such as AI, in its

commercial business and compliance program

- How a company curbs any potential negative consequences resulting from the use of technologies
- How a company is mitigating the potential for deliberate or reckless misuse of technologies, including by company insiders
- If a company is using AI in its business or part of its compliance program, whether controls are in place to monitor and ensure its trustworthiness

These changes make clear that corporations should be sure to guard against risks posed inside *and* outside their own walls by emerging technologies. On this score, Argentieri noted that prosecutors would also consider whether a company is vulnerable to AI-facilitated criminal schemes such as false approvals and other AI-generated documentation.

Here, an example not mentioned by Argentieri, but one that could apply, relates to financial institutions and other businesses subject to Know Your Customer ("KYC") laws. KYC processes may be particularly prone to the risks posed by generative AI in the form of deepfakes or other artificially manipulated documentation used to circumvent KYC safeguards against fraud, corruption, and terrorist financing. In such an instance, under DOJ's new guidance, DOJ would consider whether a victim of such attacks had compliance controls and tools in place to identify and mitigate those risks. Indeed, further reflecting DOJ's new focus on AI risks, in March 2024 Deputy Attorney General Lisa Monaco announced that DOJ will seek "stiffer sentences" against those deliberately using AI to perpetrate white collar crimes.

Implementing AI and Other Resources to Strengthen Compliance Programs

While cautioning against the risks posed by AI and other emerging technologies, at the same time DOJ indicated that companies should be leveraging their technological capabilities and other resources to advance their compliance functions. The ECCP updates reflect the Criminal Division's plans to scrutinize whether companies are using internal data, resources, and technology to effectively reinforce their compliance program in ways that are proportionate to other areas of the business. Prosecutors will consider whether a company is "appropriately leveraging data analytics tools to create efficiencies in compliance operations and measure the effectiveness of components of compliance programs."

What Does This Mean for In-House Counsel?

The updates to the ECCP show that DOJ is clearly focused on how emerging technologies—and AI in particular—are posing risks to companies and how companies are responding to those risks.

While the ECCP is designed to serve as guidance for prosecutors in making charging and resolution decisions, it can also serve as a resource for in-house counsel to assess and strengthen their corporate

policies, procedures, and risk mitigation plans. The updated guidance can be found here.