ALM | LAW.COM

New York Law Journal

WHITE-COLLAR CRIME

Get Smart or Get Indicted: Corporate Compliance in the Age of AI

By Robert J. Anello and Richard F. Albert
October 9, 2024

By **Robert J. Anello**

And **Richard F. Albert**

The Justice Department's hop onto the AI bandwagon seemed inevitable with the technology's constant buzz in the news, and alas, executives responsible for corporate compliance programs must take heed. For companies facing criminal allegations, a robust compliance program can mean the difference between an indictment and a declination. In the September 2024 update to its published guidance for the Evaluation of Corporate Compliance Programs (ECCP), the DOJ cautioned corporations to mitigate the risks of emerging technologies, such as artificial intelligence (AI), while simultaneously urging them to utilize the capabilities of those technologies in their compliance programs. The DOJ advised companies to implement processes for identifying and managing emerging technological risks; provide technological resources, such as data analytics tools, to compliance teams to maximize their efficiency and effectiveness; and closely oversee new technologies, which may be capable of causing unethical or unlawful behavior. As Deputy Attorney General Lisa Monaco remarked, the DOJ is "laser-focused on what may well be the most transformational technology we've confronted yet: artificial intelligence." Companies, C-Suites, and their legal and compliance advisers are well advised to be similarly attentive.

Why Do Corporate Compliance Programs Matter?

The holy grail of corporate compliance programs is to prevent all corporate misconduct, a quest well recognized to be unattainable. When wrongdoing inevitably occurs, the better the compliance program, the better the outcome for the corporation enmeshed in a criminal investigation or prosecution.

The DOJ's Principles of Federal Prosecution of Business Organizations direct prosecutors to assess corporate compliance programs at the time of the alleged offense and charging decision. Although counsel typically faces the difficult task of defending a program in the face of what appears to be a serious failure, under these Principles, an assessment of the quality of a compliance program is intended to have

a direct impact on key prosecutorial decisions. These include whether to charge the corporation at all; the terms of a corporate criminal resolution; and the need for an independent compliance monitor. The quality of the program also informs the amount of monetary fines, if any.

Thus, under the DOJ's Corporate Enforcement and Voluntary Self-Disclosure Policy, a company qualifies for a presumption of declination and reduced penalties if, among other criteria, the company remediates by timely modifying its compliance program. Similarly, under Section 8C2.5 of the Federal Sentencing Guidelines (Guidelines), if a corporation can show that it had an adequate compliance program at the time of the offense, it can reduce its culpability score and potential fines.

For example, in September 2024, TD Securities, the New York broker-dealer affiliate of the Toronto Dominion Bank group, entered into a Deferred Prosecution Agreement (DPA) with the DOJ in the District of New Jersey. The agreement resolved wire fraud charges against TD Securities based on alleged "spoofing" in the Treasury securities markets. TD Securities agreed to pay a monetary penalty of approximately $15.5 million. The DOJ noted that TD Securities received credit for its remedial measures, including "reviewing and continuing to enhance [its] compliance function." By contrast, in August 2024, Austal USA, a shipbuilder based in Mobile, Alabama, pled guilty to one count of securities fraud and one count of obstruction of a federal audit in the Southern District of Alabama. Austal agreed to pay $24 million in a criminal monetary penalty. Unlike TD Securities, Austal did not receive credit for its remedial measures, which were untimely and incomplete.

In short, the caliber of corporate compliance programs can often have a substantial effect on criminal resolutions. The same is true for civil enforcement resolutions with agencies like the Securities and Exchange Commission. With the stakes so high, companies will want to consider enhancing their compliance programs in light of the DOJ's new AI guidance. Tracking the three fundamental questions that the ECCP poses, this column offers suggestions for corporate compliance in a world of evolving technologies.

Is the Corporate Compliance Program Well Designed?

Under the ECCP, in evaluating a corporate compliance program, prosecutors are to first ask whether it is well designed. In the context of important new technologies, a well-designed compliance program includes a process for identifying and responding to emerging technological risks and integrating that process into the company's broader risk management scheme. A company should also establish a sound approach to governance and accountability over new technologies in both business and compliance operations; take steps to curb any negative impact, unintended consequences, or misuse of the technologies; and implement controls to ensure that the technologies are reliable, lawful, and ethical. Implementing these practices should entail pertinent updates to company policies and procedures and employee training.

A well-designed compliance program should also utilize available data to apply risk-based due diligence to third-party relationships. Although ECCP guidance on third-party relationships is nothing novel, it takes on a new meaning as companies increasingly use third-party AI tools. Moreover, "shadow AI"—unsanctioned AI use outside of IT governance—is a developing trend within organizations. Companies should closely monitor their use of AI and scrutinize the credibility of their AI partners.

Consider a recent, first-of-its-kind settlement as a cautionary tale. In September 2024, the Texas

Attorney General's (AG) Office announced a settlement agreement with Pieces Technologies, a Dallas-based AI health care company that deployed its products at four major Texas hospitals. The hospitals provided their patients' health care data to Pieces in real time, and Pieces used its AI products to summarize the patients' conditions and treatments for health care professionals. The Texas AG's investigation led it to claim that Pieces' public statements that its AI products were "highly accurate" were likely false and deceptive. As part of the settlement, Pieces agreed to accurately disclose to hospital staff its products' reliability, information about the metrics it uses to gauge reliability, and the potentially harmful uses or misuses of its products. Expected similar efforts by other prosecutors to unveil their own path-breaking AI-related enforcement actions illustrate the importance for companies to engage in thorough due diligence of third-party AI partners.

In sum, the first step prosecutors are directed to take to evaluate a corporate compliance program is to examine its design. In today's environment, a well-designed compliance program has systems for managing emerging technological risks, policies and procedures memorializing those practices, and processes for data-driven, risk-based due diligence of third-party AI tools.

Is the Corporate Compliance Program Adequately Resourced and Empowered to Function Effectively?

Next, prosecutors are directed to analyze whether the compliance program is implemented, resourced, and revised effectively. From a technological standpoint, an adequately resourced and empowered compliance program gives compliance personnel knowledge of and access to relevant data sources; maximizes the utility of data analytics tools to make compliance operations more effective; properly measures the accuracy of those tools; manages the quality of company data sources; and proportionally allocates technological resources between business operations and risk mitigation efforts.

Albemarle Corporation, a publicly traded specialty chemicals manufacturing company based in Charlotte, North Carolina, serves as a useful case study. Albemarle entered into a Non-Prosecution Agreement (NPA) with the DOJ in the Western District of North Carolina for agreeing to pay bribes to government officials in Vietnam, Indonesia, and India in violation of the Foreign Corrupt Practices Act (FCPA). Under the NPA, Albemarle received an approximate $218 million fine, which represented a record-high 45% reduction in fines from the bottom of the applicable Guidelines range. The DOJ cited Albemarle's prompt engagement in extensive remedial measures as a reason for the reduction, and in particular, its implementation of data analytics to monitor and measure its compliance program's effectiveness.

Furthermore, as part of the NPA, Albemarle agreed to ensure that compliance and control personnel have sufficient access to relevant data sources to allow for timely and effective monitoring and testing of transactions. Although the NPA does not reference AI, companies should consider how AI might facilitate their data analytics and compliance with anti-corruption laws like the FCPA, as AI has the potential to analyze large datasets and identify red flags in real time.

Thus, under the ECCP, the second inquiry that prosecutors make is whether a compliance program is adequately resourced and empowered to function effectively. To meet that standard in the digital age, companies must make use of emerging technologies. As Assistant AG Nicole Argentieri explained last year, the DOJ is "upping [its] game when it comes to data analytics," and it "expect[s]" companies to do the

same." The Albemarle NPA illustrates that the DOJ is not merely paying lip service to this topic.

Does the Corporate Compliance Program Work in Practice?

The third and final question prosecutors are to ask in evaluating a corporate compliance program is whether it works in practice. A compliance program works best in practice if it is constantly improving and evolving, and evolution is at a premium when it comes to new technologies.

If a company uses new technologies in its commercial or compliance operations, it should frequently monitor and test those technologies to determine whether they are working as intended and are consistent with the company's code of conduct. If AI or another technology drives conduct that is inconsistent with company values, the company should have a system to quickly detect and correct that conduct.

What conduct might AI suggest that contravenes company values? As the DOJ Civil Rights Division has found, it might lead to—and has led to—unlawful discrimination. Consider the hiring process as an example. Although AI can streamline that process, it also has the potential to screen out candidates in a discriminatory manner. Last year, the Equal Employment Opportunity Commission (EEOC) announced a settlement in *EEOC v. iTutorGroup*, its first lawsuit involving discrimination driven by AI tools in the workplace. The EEOC sued the defendants in the Eastern District of New York, alleging that they programmed their AI recruiting tools to automatically screen out candidates over a certain age in violation of the Age Discrimination in Employment Act. The settlement illustrates one of the many pitfalls of AI, and how it behooves companies to regularly monitor and engage with newly adopted technologies to avoid unlawful and unethical behavior.

In short, the final query prosecutors are tasked with making in assessing a corporate compliance program is whether it works in practice. For compliance programs to work in practice, companies must closely oversee, and constantly improve, their technologies.

A Shield Against the Tech Sword

Companies that do not update their compliance programs to get smart on technology risk bad outcomes if government enforcers come knocking. The DOJ has made clear that it wants companies to rise to two daunting challenges at the same time: guarding against the many risks new technologies pose while simultaneously harnessing their capabilities for good. In a speech this year, Monaco said it best: "Every new technology is a double-edged sword, but AI may be the sharpest blade yet." A thoughtfully updated compliance program can serve as a company's shield.

Robert J. Anello and **Richard F. Albert** *are partners at Morvillo Abramowitz Grand Iason & Anello.* **Grace Manning***, an associate of the firm, assisted in the preparation of this article.*