Pepper Hamilton LLP
Attorneys at Law

Lessons From the DOJ: How Recent Guidance and Cases Can Help You Avoid Government Interference With Your Business

ALERT | September 9, 2019

Callan G. Stein | steinc@pepperlaw.com
Miranda Hooker | hookerm@pepperlaw.com

The initiation of a government investigation is often a stressful and anxiety-producing event for a health care company. The Department of Justice (DOJ) is known for its aggressive investigation and prosecution of health care fraud and related offenses, and the potential penalties can have a significant impact on the livelihood and future of a company. In addition, the statutory framework is such that the DOJ can prosecute the same conduct criminally or civilly, and it can use different statutes to bring charges based on the same conduct but with dramatically different penalties. This article discusses recent

DOJ guidance and enforcement actions focused on corporate compliance programs and, based on that, identifies strategies corporations can use to develop and implement comprehensive compliance programs designed to ward off government investigations and enforcement actions.

History of DOJ Guidance on Corporate Compliance Programs

When discussing DOJ guidance on virtually any topic, the place to begin is the Justice Manual (formerly known as the United States Attorney's Manual), and the topic of corporate compliance programs is no exception. Title 9, section 28 of the Justice Manual ("Principles of Federal Prosecution of Business Organizations") addresses how the DOJ decides whether to bring criminal charges against a corporation, and, as one might expect, the existence and substance of a corporate compliance program is a critical factor in that decision.

Section 28.800 of the Justice Manual ("Corporate Compliance Programs") lists the "critical factors" the DOJ applies when making its key determinations in the evaluation of a corporate compliance program: (1) "whether the program is adequately designed for maximum effectiveness in preventing and detecting wrongdoing by employees" and (2) "whether corporate management is enforcing the program or is tacitly encouraging or pressuring employees to engage in misconduct to achieve business objectives." Put another way, the Justice Manual challenges prosecutors to determine whether a corporation has thoughtfully "designed, implemented, reviewed, and revised" its corporate compliance program or whether it, instead, merely has a "paper program" that is neither genuinely implemented nor scrupulously followed.

On April 30, 2019, the DOJ Criminal Division released a formal Guidance Document titled "Evaluation of Corporate Compliance Programs" (the 2019 Guidance). The 2019 Guidance applies to the DOJ's Criminal Division and contains extensive guidance on how the Criminal Division instructs its prosecutors to evaluate the compliance programs of corporations under investigation. At its core, the 2019 Guidance focuses on the three "fundamental questions" prosecutors ask in the course of making a charging determination: (1) Is the corporation's compliance program well-designed?; (2) Is the program being implemented effectively?; and, (3) Does the corporation's compliance program work in practice? Corporations must be able to answer these questions to the satisfaction of prosecutors because it is in the course of answering these questions that federal prosecutors decide whether they will prosecute a corporation and/or what terms of a potential resolution they are willing to offer.

Thoroughness and Creativity: Key Themes From the 2019 Guidance

The 2019 Guidance spans 19 pages and addresses virtually every aspect of the design, implementation and effectiveness of a corporate compliance program. At times, the guidance discusses very specific individual characteristics of a corporate compliance program that prosecutors expect to see. In doing so, two key themes repeatedly emerge that will help corporations satisfy their compliance obligations: (1) being **thorough** in developing and implementing your compliance program and (2) thinking **creatively** about how to address your business's specific compliance concerns.

Thoroughness

Customization: A corporation should tailor its compliance program to its specific business and industry.

The DOJ could not have more clearly conveyed in the 2019 Guidance that it expects corporations to tailor their compliance programs to the specific compliance risks they face. Put another way, the DOJ does not want to see, and will not accept as effective, cookie-cutter or "canned" compliance programs that are pulled off the internet or copied from another business.

In fact, when evaluating a compliance program, the "starting point" for any prosecutor will be determining whether the program is designed to detect "the particular types of misconduct most likely to occur in a particular corporation's line of business." This critical question embraces two different, but related, principles that every corporation should be considering: (1) the need for a corporation to conduct its own, particularized risk assessment to identify its specific risks and (2) the need to account for those risks when drafting the compliance program.

In conducting a risk assessment, the DOJ provides a list of the factors that it believes bear directly on a corporation's risk profile. They are location; industry sector; competitiveness in the market; regulatory landscape; potential clients and business partners; transactions with foreign governments; payments to foreign officials; use of third parties; gifts, travel and entertainment expenses; and charitable and political donations. A corporation should use this list as an outline when evaluating its risk profile *before* putting pen to paper to draft compliance policies, and it should document its evaluation of each risk area.

Once the company-specific risks are identified, the corporation must account for them in its compliance program. The 2019 Guidance acknowledges that not all risks are created equal. Thus, once a corporation identifies its risks, it should analyze them on a "spectrum" from the lowest-risk to the highest-risk areas. By organizing its risks in this manner, the corporation can begin tailoring its compliance policies and procedures to more specifically address the highest-risk areas first. The DOJ has stated that it wants to see corporations prioritizing higher-risk areas, and devoting proportionately more compliance resources to detection and prevention therein.

Third-Party Management: Compliance begins at home, but it does not end there, as corporations should extend their compliance efforts to third parties.

Throughout the 2019 Guidance, the DOJ makes numerous references to corporate compliance efforts extending beyond employees to third parties (vendors, contractors, consultants, etc.). In this respect, the updated guidance warns corporations to focus on compliance during all three phases of a third-party relationship: pre-engagement, during the engagement, and post-engagement.

As a threshold matter, the DOJ suggests that corporations should exercise restraint when deciding whether to engage a third party at all, and limit such engagements to situations where it is strictly necessary. On its face, whether a corporation actually "needs" to engage a third party seems to fall more in the category of "business decision" than it does "compliance decision." However, the DOJ is very upfront that it views third-party arrangements as inherently suspect: "[A]gents, consultants, and distributors are commonly used to conceal misconduct such as payment of bribes to foreign officials in international business transactions." On the one hand, it is not difficult to argue that this is an overly jaded view of third-party relationships. On the other hand, the DOJ can certainly point to myriad examples of corporations engaging in misconduct through third parties that support this belief. Regardless, this remains the DOJ's view on the subject, and corporations should heed the DOJ's clear advice and ensure their compliance program provides a mechanism for making and documenting this threshold determination of need and, more importantly, ensuring that the corporation has valid and provable justifications for all of its third-party relationships.

Once the decision that a third party is needed is made, the updated guidance focuses primarily on corporations having a system for, first, conducting sufficient initial due diligence of third parties before engagement and, second, for conducting ongoing monitoring of the

third parties after engagement. The DOJ warns that, before engaging any third party, a corporation should research its reputation in the industry and its past compliance record, and also scrutinize its existing relationships (especially with foreign officials). Any third party that does not satisfactorily pass this diligence should be disqualified. Then, even where a third-party passes through initial diligence and is engaged, the corporation has an ongoing responsibility to continue to monitor the third party to ensure no compliance issues arise. A corporation can achieve this, for example, by conducting periodic compliance audits of third parties.

Compliance Updates: A corporate compliance program should be a living, breathing organism, subject to periodic evaluations and constant improvements

Perhaps no theme resonates more throughout the 2019 Guidance than the DOJ's laser-like focus on a corporation's efforts to learn from mistakes and consistently work to improve its compliance program: "One hallmark of an effective compliance program is its capacity to improve and evolve . . . . [P]rosecutors should consider whether the company has engaged in meaningful efforts to review its compliance program and ensure that it is not stale." From this, it is fair to conclude that prosecutors will look very favorably on corporations that can demonstrate substantive, periodic updates to their compliance programs (and their internal risk assessments).

The DOJ also offers guidance on how corporations might go about identifying where compliance program updates need to be made. First, and most obviously, the DOJ points to instances of past misconduct as clear signals that a compliance program needs updating. The occurrence of misconduct, the DOJ posits, signals a breakdown in the compliance program that should be fixed to, at a minimum, prevent recurrence. This is true regardless of whether the compliance program detected the misconduct, though it is fair to assume that needed revisions to a corporate compliance program may be more obvious (and, thus, more critical in the eyes of the DOJ) in situations where the corporate compliance program failed to uncover employees' misconduct.

To ensure *all* proper revisions are made when misconduct is detected, in addition to punishing the individual offenders, the DOJ directs corporations to conduct a root-cause analysis aimed at identifying the gaps in the compliance process that enabled the misconduct to occur. Revisions aimed at filling in these gaps will demonstrate a corporation's commitment to preventing future compliance violations. In addition, the DOJ suggests corporations undertake proactive measures to identify areas that need improvement be-

fore misconduct occurs. The measures the DOJ suggests in this regard include conducting periodic internal audits of control and tracking systems and engaging with employees to identify areas of weakness.

Creativity

Customized Training: Not all compliance training is created equal, and corporations should tailor training to maximize its effectiveness.

The 2019 Guidance emphasizes the importance of compliance training, going so far as to call it a "hallmark of a well-designed compliance program." Corporations should heed this guidance and emphasize initiatives designed to creatively and effectively communicate their compliance policies to their employees (and third parties, as appropriate).

The first step in effectively communicating compliance policies to employees is, fairly obviously, to hold regular training sessions. But if a corporation simply holds traditional, run-of-the-mill training sessions, it misses an opportunity to demonstrate to prosecutors its commitment to establishing a compliance culture by customizing its compliance program to improve employee compliance training. Instead, corporations should think creatively and design custom training strategies that will maximize the attendance and comprehension of their specific workforce.

One such creative method for improving training is to vary the substance and method of delivery of training sessions based on the specific audience. For example, basic, high-level compliance training may be extremely useful for new employees who have not yet been indoctrinated into a corporation's compliance program, but it likely will be repetitive and tedious for existing, long-term employees. Instead, those employees would likely benefit more from "refresher" training sessions that focus on recent compliance events or newly revised compliance policies. A corporation may also find that it is most effective to deliver introductory training in person over the course of a half-day or full-day meeting, but to deliver refresher training over the course of several 30-minute long webinars.

Similarly, corporations should consider varying the substance of training on certain compliance topics based on their level within the organization. For example, a corporation may determine that it is more effective to train employees in supervisory roles on how to investigate and address internal reports of potential compliance issues outside the presence of their subordinates, who may one day be subject to such an investigation. If so, a corporation may hold a separate, supplemental training session exclusively for supervisors.

Corporations should also consider creative methods for assessing and, more importantly, demonstrating their employees' comprehension of the training. The tried and true method corporations have used for some time in this regard is to require employees to pass a written test or quiz at the conclusion of training in order to receive credit for it. There is little doubt this method has value, but a little creativity may yield a more effective approach for each specific workforce. For example, for certain corporations and certain types of employees, it may be effective to simulate on-the-job situations that test employees on one or more aspects of the compliance training the employee just received (similar to "secret shoppers" in a retail setting). The more a corporation does to demonstrate its commitment, not just to conducting trainings but to conducting *effective* trainings, the better off it will be.

Importance of Internal Reporting: Corporations should actively encourage internal compliance reporting to avoid creating whistleblowers.

The word "whistleblower" is enough to send shivers up the spine of most corporate executives — and for good reason. Recent years have seen whistleblower cases continue to rise, in large part due to reports of whistleblowers collecting multimillion-dollar awards as part of settlements. As a result, corporations are asking with more and more frequency how they can "identify" whistleblowers among their workforce. This is, of course, an impossible question to answer, as whistleblowers do not walk around wearing shirts bearing that label.

Rather than engaging in the guesswork of trying to *identify* whistleblowers, a more effective strategy for a corporation is to leverage its compliance program to avoid *creating* whistleblowers in the first place. There are many reasons a whistleblower may go outside the corporation to raise his or her concerns. Some reasons are outside a corporation's control *(e.g.*, the promise of a large payday), but many are not. For example, many whistleblowers complain that a corporation had no mechanism for employees to raise complaints internally, and no effective way to protect complainants from retaliation. Worse, many of the nastiest whistleblower cases include allegations that the whistleblower repeatedly raised the issues internally but was ignored by management each time.

The best way to avoid creating whistleblowers is to do everything possible to *encourage* individuals who have complaints to raise them internally, where the corporation can maintain control over the investigation. And corporations should think creatively about

how they can utilize their existing compliance programs to do so. For example, corporations should implement multiple mechanisms that allow employees to report compliance violations, including at least one that permits anonymous reporting. A common method of anonymous reporting is to set up a compliance hotline. But corporations should also consider providing alternate methods, such as a lockbox where complaints can be delivered in hardcopy form, or an email account or web portal that automatically removes the sender's identifying information. And most importantly, once these reporting systems are in place, corporations should implement a system to quickly conduct thorough internal investigations of all complaints they receive, including reviewing relevant documents and interviewing potential witnesses. Conducting good faith internal investigations that genuinely seek to verify employee reports of potential misconduct is the best way for a corporation to demonstrate to its employees that their complaints are being taken seriously, and thereby persuade them that they need not bring the complaints outside the corporation (*e.g.*, by whistleblowing to the government).

Corporations should take the same creative approach when implementing safeguards to protect against retaliation. Having a strict policy forbidding retaliation against whistleblowers is a no-brainer. But corporations should seek to enhance those protections through their actions, such as by placing, when circumstances warrant, individuals accused of misconduct (especially those in positions of authority) on administrative leave pending the completion of an investigation, or by temporarily withdrawing an accused individual's authority to impose discipline or terminate employees under his or her watch. Employees are typically very attuned to these types of actions, so even a small gesture can have a significant positive impact.

Punishments and Rewards: Corporations should use both the stick (punishment) and the carrot (incentives) to prevent compliance violations.

Consistent with the DOJ's warning that "paper programs" are not sufficient, in the 2019 Guidance, the DOJ makes clear that it expects corporations to take action to prevent compliance violations. Deterring future violations by imposing severe punishments on compliance violators (up to and including terminating them) is an obvious, and effective, strategy. But again, by stopping there, a corporation misses an opportunity to demonstrate its commitment to compliance. A corporation should implement discipline policies that empower it to craft creative and custom punishments to maximize the deterrent impact and, in at least certain circumstances, ensure it has some manner of flexibility to decide whether and how to publicize discipline among other employees.

Corporations can also prevent compliance violations by incentivizing employees to prioritize compliance. One potentially effective method for doing so is to tie some compliance metric to employee compensation or career advancement. For example, a corporation could require that employees have a clean compliance record or complete a certain amount of compliance training to be eligible to receive an annual bonus or to be considered for a promotion. Another effective method is for a corporation to include an employee's compliance-related activities or ethical leadership as a formal component of his or her annual performance appraisal, and then document how that evaluation impacted the decisions on things like discretionary raises, bonuses or promotions. This is another effective way for a corporation to demonstrate that it values compliance the same way it values more traditional metrics used to decide compensation and advancement (*e.g.*, revenue generation, productivity, etc.).

Prosecution of Individuals for Compliance Failures: Lessons From the New Wave of DOJ Prosecutions

The Rochester Drug Co-Operative and Miami-Luken Cases

In April, the DOJ announced civil and criminal charges against the Rochester Drug Co-Operative (RDC), a regional opioid distributor, and its former CEO and former chief compliance officer. At the core of the case were allegations that "RDC knowingly failed to operate an adequate system to detect, investigate, and report to the DEA suspicious orders of controlled substances." More specifically, the DOJ's allegations fell into three general categories: (1) RDC failed to report suspicious orders from its customer (pharmacies) to the DEA; (2) RDC fulfilled orders for customers despite obvious red flags identified by its compliance department; and, (3) RDC has an inadequate compliance program and overall culture of noncompliance.

Not three months later, the DOJ announced another, extremely similar case, when it brought criminal charges against another regional opioid distributor, Miami-Luken, Inc., and its former president and former chief compliance officer. The one-count criminal indictment charged the defendants with conspiracy to distribute and dispense a controlled substance, and focused on Miami-Luken's compliance failures that generally fell into the same three categories the DOJ identified in the RDC case.

The significance of these cases is twofold. First, the DOJ's decision in both cases to charge the companies' chief executive and chief compliance officers is no coincidence.

To the contrary, these cases could be a signal of the next wave of DOJ prosecutions that target the individuals responsible for a corporate compliance program when that program does not function properly. Second, and more importantly, the parallels between the allegations in both cases reveal two specific compliance failures that are clearly at the forefront when the DOJ decided to bring these cases: (1) a compliance department's failure to act when it identifies suspicious activity and (2) a corporation's failure to sufficiently empower and support its compliance function.

Actual Knowledge Plus Inaction

The most striking similarity between the two cases is the DOJ's focus on, and clear outrage over, the fact that the compliance departments of both RDC and Miami-Luken were aware of certain "red flags" identifying suspicious ordering practices by their customers but ignored them repeatedly in the name of making sales. For example, both RDC's and Miami-Luken's compliance departments red-flagged orders by pharmacies that sought volumes far in excess of the internal threshold the corporations' compliance departments had previously determined to be reasonable. This included the companies selling millions of doses of opioids to pharmacies in towns of just over 1,000 people, and selling drugs to pharmacies the compliance departments had identified as being paid in cash for the majority of their opioid sales (a known red flag when dealing with opioids).

In these instances, the RDC and Miami-Luken compliance departments initially did what they were supposed to: They identified potentially suspicious orders by applying preset metrics. The failures came after these identifications were made, when the corporations' executives chose to ignore the suspicions and fill the orders without conducting any investigation or due diligence (as required by, among other laws, DEA regulations).

The inclusion of this "knowledge plus inaction" paradigm in both cases was intentional by the DOJ. To prove criminal liability, the DOJ must establish the requisite intent of each individual to commit the crimes charged. Absent actual statements from those individuals evidencing their criminal intent (which are extremely rare in such cases), the DOJ was left to establish intent through circumstantial evidence. Proving that each individual was aware of red flags (from the compliance department) but authorized the sales regardless and without conducting any of the required investigation is precisely the type of circumstantial evidence from which a jury could infer intent because, at a minimum, it establishes that each individual acted with knowing disregard of his obligations.

Failure to Empower and Support Compliance

The other common theme across the RDC and Miami-Luken cases is the DOJ's frustration with both corporations' failure to sufficiently empower and support their compliance programs. The need for a corporation to provide proper staffing, funding and authority to a compliance department is addressed in some detail in the DOJ's 2019 Guidance (discussed earlier), and the importance of following that guidance was on full display in these cases.

Among other things, the 2019 Guidance warns that corporations should ensure their compliance departments operate autonomously, meaning that compliance personnel are sufficiently experienced to perform the function and have sufficient independence and authority to effectuate compliant conduct. Clearly, the compliance personnel who identified the suspicious orders for both RDC and Miami-Luken were not empowered at all to prevent the ultimate sales, or even delay them until an investigation was conducted. The DOJ's displeasure with this fact is clear from the allegations against both sets of the defendants, and the accompanying press releases.

In its complaint against RDC, the DOJ took this displeasure a step further by noting two facts specifically: (1) that RDC — despite having more than $1 billion in annual revenue — did not hire a dedicated compliance officer, but instead added the compliance function to an existing employee who already had "a number of other time-consuming tasks, such as managing RDC's warehouse and tracking inventory" and (2) when RDC did finally expand its compliance department, it hired unqualified personnel, including "the daughter of the company's General Manager to serve as a 'Compliance Specialist.'" Although this may appear to be after-the-fact nitpicking by the DOJ, in this case, the DOJ left no doubt that its distaste for what it perceived to be RDC's cavalier attitude toward compliance (illustrated by decisions like these) contributed to the decision to bring criminal charges against it and its two executives. Other corporations should take notice.

Substantial Compliance Changes in the Wake of Alleged Misconduct Matters

For corporations under investigation (or facing enforcement action), the DOJ has demonstrated a willingness to reward those that undertake significant efforts to remedy past misconduct. The Justice Manual (section 9-27.220) dictates that a federal prosecutor "should commence or recommend federal prosecution if he/she believes that the person's conduct constitutes a federal offense, and that the admissible evidence will prob-

ably be sufficient to obtain and sustain a conviction, unless (1) the prosecution would serve no substantial federal interest; (2) the person is subject to effective prosecution in another jurisdiction; or (3) there exists an adequate non-criminal alternative to prosecution."

The most effective area for advocacy is in the third exception: that there exists an adequate non-criminal alternative to prosecution. The Justice Manual directs a federal prosecutor to consider all relevant factors when determining whether such an adequate non-criminal alternative to prosecution exists, including: "(1) the sanctions or other measures available under the alternative means of disposition; (2) the likelihood that an effective sanction will be imposed; and (3) the effect of non-criminal disposition on federal law enforcement interests." Examples of non-criminal alternatives to prosecution are varied and include civil actions under the False Claims Act (FCA); administrative suspension, debarment or exclusion proceedings; deferred or non-prosecution agreements, and pre-trial diversion.

A company advocating against the initiation of criminal charges on the grounds that a non-criminal alternative exists can enhance its position with a health care fraud prosecutor by demonstrating substantial corporate changes, such as increased compliance and the removal of alleged bad actors, and argue that the collateral consequences of criminal prosecution (*e.g.*, permanent exclusion that would put the company out of business, layoffs of corporate personnel, etc.) outweigh the benefits. These arguments can be quite persuasive to prosecutors when there has been an effective and thorough internal investigation that resulted in significant changes within the company, and the company can credibly argue that there is no risk that the alleged misconduct will happen again.