BakerHostetler

Corporate Compliance Programs and the DOJ's Emphasis on Data Analytics: What Companies Need to Consider

By Jonathan B. New, Jimmy Fokas, Patrick T. Campbell and Bari R. Nadworny

October 2020

In recent months, the U.S. Department of Justice (DOJ) has raised expectations for companies to use data analytics to monitor the effectiveness of their compliance programs and to identify potential misconduct. By its terms, data analytics is the process of analyzing raw data in order to discover useful information to inform conclusions and decision-making. The DOJ has increasingly used data analytics to identify potential wrongdoing and has recently sent the message that it expects companies to follow suit and incorporate data analytics in their compliance programs. In June 2020, the Criminal Division of the DOJ issued revised guidance (June 2020 Guidance) about how it will evaluate corporate compliance programs, and it included specific references to the use of data analytics. U.S. Dep't of Justice, Criminal Div., Evaluation of Corporate Compliance Programs (June 2020).

Prior to the June 2020 Guidance, the DOJ had signaled its increased reliance on data analytics to identify potential wrongdoing and bring cases, especially within certain industries. During former Deputy Assistant Attorney General Matthew S. Miner's remarks at the 6th Annual Government Enforcement Institute in September 2019, he noted that the "use of data analytics has allowed for greater efficiency in identifying investigation targets, which expedites case development, saves resources, makes the overall program of enforcement more targeted and effective." Deputy Assistant Attorney General Matthew S. Miner Delivers Remarks at the 6th Annual Government Enforcement Institute (Sept. 12, 2019). In confirming the DOJ's "focus on data analytics in identifying cases," Miner wanted to let "compliance-oriented companies," particularly companies in the securities and commodities trading space, "know that this is an area of focus." *Id.* And if misconduct does occur, Miner explained, prosecutors will inquire about what the company did to analyze or track its own data resources, both at the time of the misconduct as well as at the time of a potential resolution. *Id.* The June 2020 Guidance incorporates this concept but does not limit it to the industries noted in Miner's remarks.

In evaluating corporate compliance programs, prosecutors will now inquire about what a company did to analyze or track its own data resources.

Revised DOJ Guidance on Corporate Compliance Programs

The June 2020 Guidance builds on the Criminal Division's "Ten Hallmarks of Effective Compliance Programs," issued in 2012, the elaboration on that guidance issued in February 2017, and the subsequent update issued in April 2019. The evolution of the guidance helps companies identify what the DOJ considers best practices when designing and implementing a robust compliance program. The June 2020 Guidance notes that it "is meant to assist prosecutors in making informed decisions as to whether, and to what extent, the corporation's compliance program was effective at the time of the offense, and is effective at the time of a charging decision or resolution." June 2020 Guidance at 1. The guidance also assists companies in designing an effective program with all of the hallmarks that are significant to the DOJ so that any potential misconduct is detected early or prevented altogether.

The DOJ solidified its focus on data analytics by highlighting within the June 2020 Guidance the importance of tracking and utilizing data in connection with corporate compliance programs. Within the framework of whether a corporation's compliance program is adequately resourced and empowered to function effectively, the June 2020 Guidance added a new item titled "Data Resources and Access," which poses the following questions for prosecutors: 1) "Do compliance and control personnel have sufficient direct or indirect access to relevant sources of data to allow for timely and effective monitoring and/or testing of policies, controls, and transactions?" and 2) "Do any impediments exist that limit access to relevant sources of data and, if so, what is the company doing

to address the impediments?" *Id.* at 12. The updated guidance also addresses — within the context of whether the corporation's compliance program is well designed — whether a company's risk assessment is subject to periodic review and whether that periodic review is limited to a snapshot in time or based on continuous access to operational data and information across functions. *Id.* at 3. The DOJ will also consider whether a company tracks access to various policies and procedures to understand what policies are attracting more attention from relevant employees, and whether the company periodically tests the effectiveness of its whistleblower hotline, for example, by tracking a report from start to finish. *Id.* at 4, 7.

When the DOJ offers revised guidance such as the June 2020 Guidance, it is not always immediately clear to companies exactly what modifications they should make, if any, to their compliance programs. The concept of data analytics has been a relatively recent focus for the DOJ, making it even more challenging for companies of different sizes in different industries to determine what type of data analytics tools are necessary or, at a minimum, recommended. However, the following are two areas in which companies should consider incorporating the use of data analytics in their compliance programs to meet what appears to be the expectations set forth in the June 2020 Guidance.

Testing the Effectiveness of the Compliance Program

Entities can implement certain data analytics tools to test the effectiveness of their compliance programs. One example provided by the DOJ in the June 2020 Guidance is tracking access to various policies and procedures to understand what policies are attracting more attention from employees. Many companies make their policies available via an internal company website but may not take affirmative steps to learn how frequently employees are accessing them. For example, tracking which specific policies or procedures, such as a company's anti-bribery policy or anti-retaliation policy, employees are most frequently accessing could prove useful in determining whether there are particular issues causing employees to seek guidance. Similarly, companies with whistleblower hotlines might also analyze the data surrounding when and how the hotline is accessed in an effort to understand whether the hotline is operating effectively. A company may learn, for example, that a certain business segment most frequently accesses the whistleblower hotline. Another company may learn that a specific provision of its code of conduct regarding confidential information was viewed frequently within a certain time period.

Companies can also track information learned from online training modules, including which modules are re-accessed and how regularly. This analysis is even more important in the current environment caused by the pandemic, as employees may not know they have access to these materials remotely or how to access them. Companies should ensure that all employees have ready access to compliance program policies, procedures, and training materials, and they should consider analyzing the access data set to confirm that these materials are in fact being reviewed and utilized.

The DOJ does not set forth specific recommendations regarding what to do with the data a company collects concerning its compliance program. The question posed by the DOJ is, in general, whether the company is tracking this type of data and then using the data to monitor the effectiveness of its compliance program. Thus, entities must first determine whether they already collect sufficient data to permit a meaningful analysis. Smaller entities with fewer employees may not presently generate enough data to draw conclusions. How a company analyzes the data — and whether it makes changes to its compliance program as a result of what the data shows — requires each entity to make a fact-specific determination. The goal is to make use of data analytics to monitor this more granular data set, particularly if it is readily available, and to try to make improvements when the data set shows there is room for them. The DOJ expects corporate compliance programs to adapt over time, depending on the results of internal testing and data analysis.

Identifying Red Flags

Companies should also consider how they can implement data analytics tools or enhance existing ones to identify red flags of fraudulent activity or other types of potential misconduct. Data analytics in this context will look different for different types of companies and different industries. For example, a company may consider analyzing its sales data to identify any spikes or anomalies, in particular at the end of each quarter or around other critical deadlines. Another company may consider analyzing data for expense reimbursements and payments to consultants and other third parties to monitor for activity that could constitute hidden bribes, kickbacks, or other illegitimate payments. Companies seeking to implement data analytics for the purpose of identifying red flags must think through the specific and perhaps unique red flags for the entity and the industry as a whole and whether the analysis of certain data will help identify them.

Moreover, the June 2020 Guidance maintains the DOJ's emphasis on risk-based compliance. In determining which types of red flags to address, businesses should continue to apply a risk-based approach. That same risk-based approach should be extended to decisions about where businesses should focus their data analytics efforts. Companies are not expected to search through all of their systems and platforms to find issues to research in the data. They should be aware of the risks to their business and in their industry and tailor the review of data to those specific risks. Based on these identifiable and understood risks, data analytics should be used as a tool to better inform companies and identify misconduct if it occurs.

Again, the COVID-19 pandemic makes this type of data analysis more important. Employees still are not interacting face to face, do not have regular access to their offices, and may be receiving or sharing electronic information outside the normal course of work. The remote work environment might also generate additional data as employees rely on remote technology to conduct their day-to-day duties. These factors, along with the economic pressures companies are facing as a result of the pandemic, may increase the chances of fraudulent conduct. Companies can use data analytics to address these new compliance risks during a time when the remote/hybrid working environment makes traditional compliance monitoring more difficult.

As with using data to test the effectiveness of a compliance program, questions will arise regarding a company's obligations to collect and analyze data it has never collected or analyzed before, and what a company with limited resources should do. The June 2020 Guidance confirms what has always been true: There is no one-size-fits-all approach to compliance. The DOJ recognizes that each company's risk profile and solutions to reduce its risks warrant particularized evaluation. Accordingly, the DOJ considers factors including a "company's size, industry, geographic footprint, regulatory landscape, and other factors, both internal and external to the company's operations, that might impact its compliance program." June 2020 Guidance at 1. This kind of particularized approach is relevant to the use of data analytics just as it is to compliance programs more generally. As a result, the DOJ will be more likely to expect a company with significant resources, and that generates a significant volume of data, to collect and analyze this information for compliance purposes. A smaller company with limited employees and resources may not be expected to have as robust a program for analyzing data or to generate sufficient data to permit analysis, and the DOJ will take that distinction into account.

Conclusion

Companies should consider implementing data-gathering processes to the extent they are not already in place. Once that data is collected, companies should then examine the data that their business activities and existing compliance programs generate and determine how the data can be used to enhance corporate compliance efforts. The DOJ takes a particularized approach when analyzing a corporate compliance program, and companies should similarly employ a particularized approach — taking into account size, resources, identified risks, previously collected data, and other factors — when determining where and how data analytics fits in with compliance efforts. Using data analytics helps a company demonstrate its compliance program is effective, but also helps prevent the consequences that inevitably follow when potential misconduct is left unchecked.

*****

Jonathan B. New, **Patrick T. Campbell** and **Jimmy Fokas** are partners in the New York office of BakerHostetler's White Collar, Investigations and Securities Enforcement and Litigation Team. Mr. New is also a member of the Board of Editors of this newsletter. **Bari Nadworny** is an associate in BakerHostetler's New York office.

The views expressed in this article are those of the authors and not necessarily those of BakerHostetler or its clients.

09.10.20.12.52_p04