CEP Magazine - March 2020
The role of data analytics in regulatory inquiries

By Steven Neuman and Joshua Dennis

Steven Neuman (sneuman@stoneturn.com) is a Brazil-based partner at StoneTurn, with significant expertise conducting work on the ground in Brazil and throughout Latin America. **Joshua Dennis** (jdennis@stoneturn.com) is a partner at StoneTurn, working with clients and counsel on issues requiring complex data analysis.

The Department of Justice (DOJ) has recently made clear that it will consider a company's use of data in its investigations into potential misconduct, such as violations of the Foreign Corrupt Practices Act[1] (FCPA). Specifically, prosecutors will assess whether a company's compliance department had access to internal data and whether this data was sufficiently analyzed before and during investigations in a way that would enable the detection of misconduct.

In a speech at a compliance and ethics conference,[2] The DOJ went so far as to recognize that data analytics "expedites case development [and] saves resources," and put all organizations on notice that the Justice Department is tackling enforcement with a "data-driven approach."

This focus on data analytics was also part of the April publication, the *Evaluation of Corporate Compliance Programs Guidance*.[3] The guidance itself offers no explicit details as to the data evaluation steps that the DOJ will take, but rather refers to it as an "evolving narrative arc" of the investigative process, leaving the interpretation and practice up to each company to build out for itself.

Whether as part of in-house analytic teams or through collaboration with external forensic data scientists, government agencies—such as the U.S. Securities and Exchange Commission (including the Division of Economic and Risk Analysis and the Office of Compliance Inspections and Examinations) and the U.S. Financial Industry Regulatory Authority, Brazil's Federal Prosecution Service and Office of the Comptroller General, and the UK's Financial Conduct Authority—are scrutinizing all sorts of underlying business data and delving far beyond the executive data summaries typically provided as part of an initial inquiry response.

How can companies get ahead of the new expectation?

Considering global regulators' recent interest in the data analytics area, companies would be well-served to leverage their own information across all phases of the compliance life cycle.

Pre-incident

The first step is for the company to understand all sources of data at its disposal (both internally generated and from external third parties), as well as any potential limitations to those sources. This step is critically important to ensure the company has access to all of its information, particularly in large or multinational organizations that may rely on a range of disparate systems.

The company should also conduct periodic audits to help ensure *data integrity*, meaning that the data is complete, accurate, and there are sufficient internal controls to prevent undocumented alterations or deletions. With this

foundation in place, the company can then determine, as the regulator will likely do, how these sources can be best employed through the use of data analytics to enhance the company's compliance program.

A compliance department might also consider applying data analytics in the context of its risk or gap assessments, and strengthen both preventive and detective controls. For example, a data analytics model could be used to pressure test the thresholds of a time-and-expense policy or identify meaningful shifts in spend by category or vendor. Once a potential high-risk area is identified, data analytics could make use of additional models to help determine the potential effect each might have on the business.

A data-driven assessment will help reveal the high-risk areas to consider for pre-incident monitoring, which is an important step in detecting potential misconduct. The compliance department may also consider using targeted predictive analysis as part of its monitoring program to identifying potentially problematic transactions, such as those involving foreign officials or brokers, at or near real-time.

During an incident

When potential misconduct has been identified, the pursuant forensic investigation can also be enhanced with data analytics. In many cases, employing an automated, data-driven approach can replace manual review processes that may be otherwise limited by time and resource constraints. These data analytics tools, which include the use of dynamic visualizations and dashboards, will expose patterns and outliers that can bring clarity to a suspected or alleged malfeasance. Achieving a clear trend analysis result is crucial to understanding the scope of the potential misconduct and developing an action plan for detailed transaction testing.

Importantly, data analytics tools can also help with the sample selection process by allowing a user to quickly and efficiently navigate large amounts of data to pinpoint transactions that meet certain criteria. Again, this step is a key element for completeness, so compliance professionals should make informed selections that will be further investigated to achieve full coverage over the potential misconduct.

Post-incident

Following an investigation, a root cause analysis, as well as an internal controls assessment and enhancement, should be carried out to defend against a similar breach. Data analytics can again be applied in this phase to drill down on the original control gap that allowed the misconduct to take place, and then ensure sufficient remediation through controls enhancements and testing.

An interesting application of data analytics is the "look-back capability." This technique makes it possible to determine if the same misconduct would have occurred in a different set of circumstances. For example, a company can test if a new clause in its time-and-expense policy would have prevented or detected an expense fraud scheme from occurring. Such an analysis would provide the compliance department with invaluable insight into the effectiveness of a draft policy before putting time and resources into rolling out the requirements company-wide.

Companies cannot afford to neglect data analytics

The DOJ's September remarks frame the value of data analytics succinctly: "Whereas we are able to identify indicators and anomalies from market-wide data, companies have better and more immediate access to their own data. For that reason, if misconduct does occur, our prosecutors are going to inquire about what the company has done to analyze or track its own data resources—both at the time of the misconduct, as well as at the time we are considering a potential resolution." Clearly, the use of data analytics will provide the very type of effective and sufficiently sophisticated "surveillance systems" that regulators are keen to see in place. More

importantly, data analytics tools can help counsel and in-house professionals conduct investigations more efficiently, and allow professionals to focus their time on identified risk areas and addressing potential misconduct to reduce compliance breaches overall.

Acknowledgments

Carrie Meneo, a senior consultant at StoneTurn, contributed to this article.

Takeaways

- Prosecutors are increasingly interested in a company's data, so the Department of Justice will expect compliance officers to know and effectively use the data available to them.
- Companies must take care to design and implement data analytics tools within an effective compliance program to prevent and detect potential misconduct.
- Regulatory technology is expected to make up more than one third of compliance spending by 2020.[4]
- Companies should ensure that they have effective controls over data integrity within all data sets.
- Data analytics tools undoubtedly reduce compliance breaches and increase efficiency within the department, allowing compliance and internal audit professionals to effectively manage identified risk areas.

1 15 U.S.C. §§ 78dd-1, et seq.
2 DOJ, "Deputy Assistant Attorney General Matthew S. Miner Delivers Remarks at the 6th Annual Government Enforcement Institute," speech, September 12, 2019, http://bit.ly/35ha8u2.
3 DOJ, Criminal Div., *Evaluation of Corporate Compliance Programs* (Updated April 2019), http://bit.ly/2Z2Dp8R.
4 Susannah Hammond and Stacey English, *Cost of Compliance Report 2019: 10 years of regulatory change*, Thomson Reuters, 2019, http://bit.ly/2ZJENik.