

[Blogs](#)

September 24, 2019

DOJ Leveraging Data Analytics To Detect Fraud



The DOJ is increasingly using a "data focused approach" to identify economic crime and corporate misconduct, according to a DOJ official.



In [remarks](#) to the 6th Annual Government Enforcement Institute, Deputy Assistant Attorney General Matthew S. Miner recently shared that using data analytics to identify fraud improves efficiency, expedites case development, and makes program enforcement "more targeted." While Miner indicated that data analytics are being utilized across the DOJ's white collar enforcement efforts, he pointed to the healthcare industry and financial sector as two such targets of the DOJ's data-driven enforcement approach. The DOJ has already successfully used Medicare claims data to identify fraud. That success is attributed, in part, to the DOJ's [healthcare data analytics team](#) which analyzes the Centers for Medicare and Medicaid Services' payment database for health care fraud activity and trends. The financial sector—specifically the commodities and securities arena—represents an expanding "area of focus" for the DOJ's data-driven enforcement. Miner indicated that the DOJ uses trading data to identify indicators or anomalies that are suggestive of market manipulation and other fraudulent activity. Given the DOJ's own emphasis on data-driven enforcement, Miner

encouraged companies to "analyze or track [their] own data resources." In particular, Miner noted that while the DOJ has access to market-wide data, a company can more quickly marshal its own data to detect fraud. Miner emphasized that when fraud is identified, the DOJ will be asking companies how they analyzed or tracked their data at the time of misconduct and thereafter. Such inquiries by the DOJ into the ways in which companies use data to detect fraud are consistent with other recent guidance provided by the DOJ. For example, in its [April 2019 guidance, "Evaluation of Corporate Compliance Programs,"](#) the DOJ advised that one of the ways in which prosecutors should assess the effectiveness of a company's compliance program is by identifying the "information or metrics . . . the company collected and used to help detect the type of misconduct in question" and "how [that] . . . information or metrics informed the company's compliance program." While it is not always clear which data is being tracked or analyzed by the DOJ to detect fraudulent activity, that should not deter companies from considering how they can use analytics to proactively identify harbingers of potential fraud. Of course, undertaking such efforts implicates important financial and legal considerations. First, the financial resources required to develop and implement data monitoring can be considerable, especially for companies that are not otherwise maintaining extensive databases, or deal with vast data sets—like trading data. Second, any time a company looks to expand its data pool, it should assess the regulatory implications in doing so. For multi-national companies, amassing such information can trigger a host of domestic and international data security and privacy obligations, particularly for healthcare-related data. Nonetheless, for companies operating in targeted and high-risk industries, the efforts entailed in optimizing their self-monitor capabilities may bolster their compliance programs and help them get ahead of (or on equal footing with) enforcement officials who are likely already mining their data to detect misconduct.

Authors

Explore more in

[White Collar & Investigations](#)