Published on *The National Law Review* https://natlawreview.com

Big Data: The Next Frontier in CARES Act Fraud Detection

Article By:

David L. Douglass

Jonathan E. Meyer

Charles L. Kreindler

A. Joseph Jay, III

Fatema K. Merchant

In an effort to combat the devastating economic effects of the COVID-19 pandemic, Congress enacted the Coronavirus Aid, Relief, and Economic Security (CARES) Act, authorizing $2.2 trillion in relief—the largest stimulus package in American history. Unsurprisingly, given the magnitude of the package, the Government early on expressed a commitment to aggressively investigate and prosecute any fraud against the relief program. Beyond the scale of the expenditure, its exigency necessitated relaxed anti-fraud measures and de minimus oversight relating to distribution of funds—conditions that will keep both the Government and private relators (i.e., whistleblowers) busy over the next several years. One toolset likely to be relied upon in the coming years in connection with combatting CARES Act fraud will be data analytics and data mining.

Last week, Brian Rabbit, the acting heard of the Department of Justice's (DOJ) Criminal Division reiterated the DOJ's commitment to aggressively pursue and prosecute CARES Act-related fraud. To date, the DOJ has already charged 57 people with fraudulently obtaining more than a combined $175 million in loans through the CARES Act's Payroll Protection Program (PPP), an initiative that authorized Government-backed loans to help businesses cover expenses during the slowdown brought on by the coronavirus pandemic. In doing so, Rabbit commented that the fraud section has used data analytics to bring a glut of fraud cases within mere months of the PPP's launch.

This is no surprise. The use of data analytics to pursue Government fraudsters is not new, though the Government and private relators are getting more sophisticated. Litigation trends in the prosecution of False Claims Act (FCA) cases, for example, has been increasingly data-driven over the past decade. The Government and relators have been relying on advanced data mining and analytics techniques to spot indicators of fraud (or anomalies in the data) in publicly available data sets. Back in 2011, the Centers for Medicaid and Medicare ("CMS") decided to anonymize and publicly release Medicare claims data to promote transparency in connection with the costs of healthcare. Relators have exploited this data by applying proprietary data mining and analytics techniques to identify anomalies in this and other public data sources, in order to pursue lucrative FCA judgments. In fact, a number of recent FCA lawsuits were filed by corporate data analytics whistleblowers with no other connection with the defendant.1

This trend is not limited to the private bar—the DOJ has also adopted these technologies. In fact, the DOJ has created a dedicated Office of Data Analytics (the Office), specifically charged with detecting fraud and supporting the DOJ,

Office of the Inspector General, Federal Bureau of Investigation, and other sub-agencies within the DOJ. The Office, though still relatively new, has already proven quite effective. After pulling and examining data from Medicare, Medicaid, the Centers of Disease Control and Prevention, state pharmacy data, and other sources, the Office facilitated the massive Government crackdown on opioid over-prescription in response to the nationwide crisis.

The DOJ's reliance on data analytics in connection with the CARES Act investigations and prosecutions is likely to increase, as Rabbit suggested. So too will the amount of data the Government will have to draw from and, given that the data are created by companies that are already resource-strained, so too will data anomalies and errors. What the Government's final strategy to overcome these technical challenges remains to be seen. One component already being piloted is significant internal coordination across various agencies and divisions of the federal Government, with the goal of pooling and unifying disparate pockets of technical expertise. For example, the Securities and Exchange Commission has been focused on enhancing its data analytics programs over the last year. Both the IRS and the Federal Communications Commission also have developed substantial experience in data mining in the context of their own enforcement actions. We have already seen coordinated investigations of CARES Act prosecutions with the Small Business Administration—Office of Inspector General, the IRS, the SEC, and the FBI. Such coordination will likely extend to encompass additional parts of the Government with this crucial technical expertise.

In the wake of this increased focus on data, companies should continue (or start) to leverage their data and metrics to pressure test their compliance programs now. The DOJ and regulators have been urging companies to do for some time, and it is clear that these types of technological and data-driven monitoring controls are going to be increasingly important. Indeed, the DOJ's current guidance asks what a company is doing in order to analyze its data for "patterns of misconduct or other red flags for compliance weaknesses." The amount, type, and depth of data will vary by industry and size of the company. Identifying various sources of operational data that can be put to use, ensuring and testing its reliability, and utilizing that data will be critical to building (and maintaining) a well-implemented data monitoring system. However, a well-implemented system alone, is not enough – in fact, corporations should take care to ensure that the system itself does not turn into a liability. Once directives are put into place for tracking the data, the output and reporting should be properly monitored and escalated to the relevant stakeholders for resolution and/or remediation. Given the Government's focus and a relator's incentives, companies will be well served to invest the resources required to identify and address issues internally first before they become compounded liabilities later.

It is equally important for companies to also recognize, however, that data never tells the whole story, especially with respect to the FCA. Yet, the Government's reliance on data to identify and investigate suspected health care fraud reveals that it all too often makes precisely this mistake; it assumes that unusual or aberrant data alone is proof of fraud. Data tells what happened but rarely why. The danger is that the data shapes the Government's view and that all subsequent investigation is tainted by confirmation bias, the tendency to view neutral facts as confirming pre-existing views. The effect can be to harden the Government’s view and make it resistant to alternative, innocent explanations.

Thus, when confronted with an allegation of fraud founded on data analysis, it is imperative to respond quickly and aggressively. Additional data and information that can correct a mistaken interpretation of the data should be identified. It is important to recognize that despite the Government’s resources, the company often has more accurate information. The Government’s data must be presented in the correct context, preferably earlier in the investigation before the Government’s becomes wedded to a mistaken view. If the information cannot be gathered quickly, consideration should be given to having an initial discussion with the Government to create space to gather the information necessary to present the data accurately. The Government will often agree to provide additional time. After all, it does not want to waste its limited investigative resources on misinterpreted data. Conversely, failing to engage constructively with the Government can cause it to conclude that there is no innocent explanation and misinterpret later efforts to explain the data as a mere defense tactic. In sum, while data certainly can be a critical element in investigating fraud, over reliance on data as evidence of fraud, to the exclusion of explanatory information, can present a serious enforcement risk to a company. That risk, however, can be managed, if addressed promptly and effectively.

Footnotes

See, e.g., U.S. ex rel. Integra Med Analytics LLC v. Baylor Scott & White Health et al., 17-CV-0886 (W.D. Tex.); U.S. ex rel. Integra Med Analytics LLC v. Providence Health Services et al., 17-CV-01694 (C.D. Cal.).

National Law Review, Volume X, Number 261

Source URL:https://natlawreview.com/article/big-data-next-frontier-cares-act-fraud-detection