August 2026

Follow us on LinkedIn

Compliance Update

DOJ's Fraud Division Announces Its Priorities and Deepens the Department's Focus on Data Analytics

By Brad Bondi, Jay Darden, Roberto J. Gonzalez, Patrick Hein, Sam Kleiner, Corinne A. Lammers, Kwame J. Manley, Leo Tsao, Jane H. Yoon and Thomas Jordan

Introduction

On August 13, 2026, Assistant Attorney General Colin M. McDonald issued a memorandum setting out enforcement priorities for the Department of Justice's National Fraud Enforcement Division (the Fraud Division). The memorandum identifies substantive priority areas, but its account of *how* the division will pursue cases is equally significant. The memorandum states that "we are building the most sophisticated, innovative, and data-driven white-collar law enforcement component in the world" where prosecutors will be supported by a "cross-disciplinary team of experts in data science, and cutting-edge technology and resources."[1]

Below, we discuss the Fraud Division's priorities, how DOJ is leveraging data analytics and artificial intelligence (AI), and practical takeaways for companies. As DOJ bolsters its data analytics capabilities, companies should consider how they can enhance their own use of data to identify and mitigate compliance risks.

The Fraud Division's Priorities

The August 13 memorandum frames the Fraud Division's mission as prosecuting "fraud in the United States, no matter its size or complexity." Prosecutors are directed to focus on frauds threatening "the health, safety, security, and prosperity of Americans." The memorandum identifies the following priorities:

- *Procurement/Public Benefits Fraud*. Procurement fraud, including defective pricing, bid rigging, self-dealing, bribery, product substitution, billing fraud, and fraud on benefit and grant programs from student loans to disaster relief to small business programs.
- *Healthcare Fraud*. Telemedicine schemes, Medicare and Medicaid fraud, controlled substance diversion, home health and hospice schemes, and deceptive marketing of unsafe products.
- *Tax Fraud*. Unethical return preparers, concealed income, abusive scheme promoters, and tax offenses layered onto program fraud.
- *Trade-Related Fraud*. Criminal trade enforcement through the Trade Fraud Task Force targeting illicit transshipment, country-of-origin fraud, undervaluation of imports, sanctions evasion, and forced labor schemes.

Notably, prosecutors are directed to "prioritize anti-fraud corporate enforcement."

In discussing each priority area, the Fraud Division also makes clear its focus on the use of data analytics, emphasizing that it will provide "greater resources, data analytics support, and best-in-class technology" to prosecutors and focus on "breaking down data barriers and eliminating silos."

The Fraud Division's Data Analytics Focus Builds on Initiatives Across DOJ

The memorandum's emphasis on data analytics builds on prior efforts in both the Criminal Division and the Civil Division to utilize data analytics to identify and build cases.

Criminal Division: In November 2023, the Acting Assistant Attorney General for the Criminal Division emphasized in a speech that from "healthcare fraud to procurement fraud to our use of 10b5-1 data and trading plans in the securities space, the Criminal Division has long been an innovator in using data to enhance its investigations and prosecutions" and that prosecutors continue to innovate in the data analytics space. Most notably, the Health Care Fraud Unit describes itself as "a leader in using advanced data analytics and algorithmic methods," with "dedicated data analysts work[ing] with prosecutors," an approach that "has led to some of the Fraud Section's largest cases and initiatives."[2] Indeed, the Criminal Division's use of claims data goes back as far as 2007 with the initial creation of the Medicare Fraud Strike Force, which was the precursor of today's much larger Health Care Fraud Unit that is now under the Fraud Division. On April 30, 2026, the Fraud Division announced the West Coast Health Care Fraud Strike Force, leveraging resources from the Northern District of California, a healthcare technology hub, and the Districts of Arizona and Nevada, where data analytics have helped reveal significant fraudulent schemes. Additionally, in the securities fraud arena, DOJ has pursued "a data-driven initiative led by the Criminal Division's Fraud Section (recently renamed to the White Collar and Corporate Enforcement Section) to identify executive abuses of 10b5-1 trading plans."[3]

Civil Division: The Civil Division also has emphasized data analytics in how it engages with *qui tam* relators who bring claims under the False Claims Act. On April 30, 2026, it announced the Fraud Oversight through Careful Use of Statistics (FOCUS) initiative in response to the "record number" of *qui tam* complaints being filed and solicited engagement with those "data miners" who analyze publicly available government data for fraud signals, file *qui tam* complaints and "demonstrate an insightful application of sophisticated technological capabilities."[4] The Assistant Attorney General of the Civil Division stated that "[s]ophisticated data analytics have become an increasingly important means of identifying fraud trends and uncovering patterns of misconduct across federal programs."

Data Analytics From Case Generation to Investigation

Data analysis can perform two functions in the context of investigations. The first is case generation: Prosecutors and analysts comb government-held and publicly available data to identify outliers that diverge enough from a peer group to warrant investigation. That analysis does not prove wrongdoing, but prosecutors may leverage it in deciding what and where to investigate further. Second, once a case is opened, prosecutors may then obtain the target company's data, analyze it with granularity, and integrate its analysis into the development of a case.

A recent conviction shows how data can be utilized for case generation. On May 18, 2026, a jury in the Central District of California convicted a physician in a $45 million scheme to defraud Medicare by billing for Botox injections that were never provided or medically unnecessary. DOJ touted that "[t]he investigation was initiated as a result of a referral from the Health Care Fraud Section's Data Analytics Team, after its analysis showed that the defendant was paid more by Medicare for Botox injections than any other doctor in the United States."[5] The analytics identified her as "an extreme outlier among doctors receiving Medicare payments for Botox." What started with identifying an outlier in the data ultimately led to an indictment and conviction at trial.

Once an investigation begins, in addition to interviewing employees and obtaining the company's documents, prosecutors may seek to collect and analyze troves of the company's data to develop their case. DOJ already utilizes a data platform that "houses data collected in the course of civil and criminal investigations." The platform "integrates data of any size or format, indexes and models the data into a unified format" that prosecutors and data scientists can use to "produce analytic work products" for various purposes, including "case theory investigations."[6]

During the course of an investigation, a review of the target company's own data can be used to tell a story about its compliance program. Prosecutors even can analyze data in ways that the company has not thought of, or is beyond industry practice, to paint a derogatory picture. Ultimately, DOJ may assess how a target company's compliance program utilized (or failed to utilize) the company's own data. In 2023, the Acting Assistant Attorney General of the Criminal Division noted that "if misconduct occurs, our prosecutors are going to ask what the company has done to analyze or track its own data — both at the time of the misconduct and when we are considering a potential resolution."[7]

How DOJ Is Leveraging AI To Augment Data Analytics

DOJ is also in the process of using AI to augment its data analytics capabilities. In its 2025 inventory of AI use cases, an annual public report, DOJ highlighted a significant increase in its use of AI and included several relevant examples.[8] DOJ, for instance, described tools that were still in pre-deployment that could (i) "apply AI-enabled anomaly detection" over Medicare and Medicaid claims data to produce "fraud risk scores, anomaly alerts, pattern classifications" or (ii) "identify[] and prioritize[e] financial fraud activity tied to open criminal investigations by including a broader data set and across multiple judicial districts to develop a better whole-of-U.S. picture of financial fraud."[9] These types of AI-based tools, once deployed, will enable prosecutors to more efficiently analyze large swaths of data to identify the types of anomalies that can lead to investigations.

It is also likely that DOJ will build on its data analytics tools to utilize AI to more effectively and rapidly analyze data and documents obtained from companies during the course of an investigation. For example, DOJ's AI inventory noted that DOJ has deployed a tool for the "integration and analysis of case information" that can produce "reports, narratives, and summaries" of the factual information gathered in cases.

Key Takeaways

Given the Fraud Division's focus on "corporate misconduct," companies should review their exposure to key priority areas, including procurement and government benefits fraud, healthcare fraud, tax fraud, and trade-related fraud.

The Fraud Division's focus on data analytics underscores the importance of the effective use of data in a company's compliance program. The DOJ Criminal Division's Evaluation of Corporate Compliance Programs (ECCP) directs prosecutors to consider whether companies are "leverag[ing] data analytics tools to create efficiencies in compliance operations."[10] As part of compliance presentations to prosecutors in the Criminal Division, companies typically describe their efforts to test and monitor the effectiveness of their programs. Data analytics provides the foundation for many of these testing and monitoring activities.

Critically, a company's own data analytics tools may discover misconduct before prosecutors do, allowing the company to terminate the conduct, implement remediation, and consider whether it wants to pursue a voluntary self-disclosure.

Companies, especially those with potential exposure to the Fraud Division's priority areas, should consider taking steps, including:

- **Ensure resource proportionality between business and compliance**. DOJ prosecutors will compare the data tools and technology available to compliance against those used by commercial operations. The ECCP emphasizes "proportionate resource allocation" between the compliance and business function, and the Criminal Division's leadership have noted that, in an investigation, prosecutors will "consider whether companies are putting the same resources and technology into gathering and leveraging data for compliance purposes that they are using in their business."[11] For example, a company that robustly utilizes AI in its business but does not make the technology available to the compliance program could be criticized by DOJ for having an under-resourced compliance program.

- **Measure the accuracy of compliance analytics**. The ECCP asks how a company is "measuring the accuracy, precision, or recall of any data analytics models it is using." Companies should document their review of compliance's data analytics program and how they remediate any deficiencies. Such review should be conducted at the direction of counsel to the extent possible to shield it from disclosure under the work-product doctrine. Prosecutors can and do request records of compliance auditing, monitoring and investigations to understand whether and when these functions previously detected the issues or subjects under review and whether and how companies responded to these prior signals or incidents. Where possible, testing whether a data analytics program would have caught specific misconduct or red flags can be a useful exercise.

- **Map compliance's access to material data**. Using a risk-based approach, catalog the company's data repositories and determine whether the compliance program has access to data that is material to its needs. The ECCP emphasizes that a compliance program should have "access to relevant sources of data to allow for timely and effective monitoring and/or testing of policies, controls, and transactions." To evaluate this issue, DOJ prosecutors have asked companies to describe the data sources that provide inputs for testing results in order to pressure test the reliability and comprehensiveness of those inputs. Data that the company possesses but is not being monitored from a compliance perspective can present risks. Where appropriate, documentation of decisions to not use particular data in a compliance program, and why those decisions were made, can help mitigate these risks.

- **Benchmark the company's data to detect anomalies**. Perform the type of peer comparisons a prosecutor or *qui tam* relator would run on publicly available data, and apply anomaly detection to internal data. Where results identify the company as an outlier on a material metric, the company should understand the reason and, where appropriate, investigate and address it.

- **Review anomalies**. When analytics reveal a material anomaly, use a risk-based approach to consider opening reviews to assess whether there is potential misconduct. Given that analytics may identify a large number of potentially problematic transactions or activities to review, companies may need to establish a review protocol and identify sufficient resources to support any reviews. Companies should consider whether all or certain reviews should be conducted as a privileged investigation directed by counsel. A capable analytics program may identify issues before prosecutors do, preserving the company's ability to consider a voluntary self-disclosure. As we discussed in a prior client alert, under DOJ's Corporate Enforcement Policy prosecutors may issue a declination where a company voluntarily self-reports misconduct and takes steps to remediate the issue.[12] Data analytics, supplemented by privileged investigations, may help companies detect potential misconduct and consider whether self-disclosure is appropriate.

DOJ is heightening its focus on data analytics as a tool for identifying misconduct. Companies, especially those that may face investigations from the Fraud Division, should stay a step ahead by improving their own data analytics capabilities as part of their compliance efforts.

✧ ✧ ✧

If you have any questions concerning these developing issues, please do not hesitate to contact any of the following Paul Hastings lawyers:

Brad Bondi
+1-202-551-1701
bradbondi@paulhastings.com

Jay Darden
+1-202-551-1961
jaydarden@paulhastings.com

Roberto J. Gonzalez
+1-202-551-1815
robertogonzalez@paulhastings.com

Patrick Hein
+1-415-856-7065
patrickhein@paulhastings.com

Sam Kleiner
+1-212-318-6232
samkleiner@paulhastings.com

Corinne A. Lammers
+1-202-551-1846
corinnelammers@paulhastings.com

Kwame J. Manley
+1-202-551-1962
kwamemanley@paulhastings.com

Leo Tsao
+1-202-551-1910
leotsao@paulhastings.com

Jane H. Yoon
+1-212-318-6006
janeyoon@paulhastings.com

Thomas Jordan
+1-202-551-1926
thomasjordan@paulhastings.com

[1] Dep't of Justice, Memorandum from Assistant Attorney General Colin M. McDonald, The Fraud Division's Enforcement Priorities (Aug. 13, 2026), https://www.justice.gov/opa/media/1457756/dl?inline.

[2] Dep't of Justice, Health Care Fraud Unit, https://www.justice.gov/criminal/criminal-fraud/health-care-fraud-unit.

[3] Press Release, Dep't of Justice, Former Chairman and CEO of Publicly Traded Health Care Company Sentenced to 42 Months in Prison for Insider Trading (June 23, 2025), https://www.justice.gov/opa/pr/former-chairman-and-ceo-publicly-traded-health-care-company-sentenced-42-months-prison.

[4] Press Release, Dep't of Justice, Civil Division Announces FOCUS Initiative for Data Miners Filing Qui Tam Complaints (Apr. 30, 2026), https://www.justice.gov/opa/pr/civil-division-announces-focus-initiative-data-miners-filing-qui-tam-complaints.

[5] Press Release, Dep't of Justice, California Doctor Convicted of $45M Botox Fraud Scheme Targeting Medicare (May 19, 2026), https://www.justice.gov/opa/pr/california-doctor-convicted-45m-botox-fraud-scheme-targeting-medicare.

[6] Dep't of Justice, Privacy Impact Assessment for USAPDAP (May 21, 2025), https://www.justice.gov/opcl/media/1427686/dl.

[7] Acting Assistant Attorney General Nicole M. Argentieri, Keynote Address at the 40th International Conference on the Foreign Corrupt Practices Act (Nov. 29, 2023), https://www.justice.gov/archives/opa/speech/acting-assistant-attorney-general-nicole-m-argentieri-delivers-keynote-address-40th.

[8] Dep't of Justice, AI Use Case Inventory, https://www.justice.gov/ai/ai-inventory.

[9] *Id*.

[10] Dep't of Justice, Evaluation of Corporate Compliance Programs (updated Sept. 2024), https://www.justice.gov/criminal/criminal-fraud/page/file/937501/dl. The Criminal Division has issued the ECCP and it remains to be seen if the Fraud Division utilizes it in conducting corporate investigations.

[11] Dep't of Justice, Principal Deputy Assistant Attorney General Nicole M. Argentieri Delivers Remarks at the Society of Corporate Compliance and Ethics 23rd Annual Compliance & Ethics Institute (Sep. 23, 2024), https://www.justice.gov/archives/opa/speech/principal-deputy-assistant-attorney-general-nicole-m-argentieri-delivers-remarks-society.

[12] Paul Hastings, DOJ's National Security Division Issues Its First Corporate Declination Under New Corporate Enforcement Policy (June 29, 2026), https://www.paulhastings.com/insights/client-alerts/dojs-national-security-division-issues-its-first-corporate-declination-under-new-corporate-enforcement-policy.