



Apr 16, 2026

Categories:
[Publications](#)

Authors:
[Logan W. Koehring](#)
[Ricardo Solano, Jr.](#)
[Robert C. Webb](#)
[R. Kent Westberry](#)

A Warning and a Roadmap: DOJ Enforcement Actions Will Come Faster, Be Better Coordinated, and Rely Heavily on Advanced Analytics

On April 7, 2026, the U.S. Department of Justice (DOJ) announced the creation of the National Fraud Enforcement Division, which marks a significant structural and strategic shift in how the federal government will approach fraud involving taxpayer dollars. The result? A more centralized, better-resourced, and increasingly aggressive enforcement environment.

By consolidating existing units such as the Criminal Division's Tax Section, Health Care Fraud Unit, and Market, Government, and Consumer Fraud Unit under a single division, the DOJ is making clear that fraud against government programs — large or small — will be treated as a top-tier enforcement priority. This realignment raises the likelihood that investigations will be identified earlier, prosecuted more consistently across districts, and pursued with greater coordination between criminal and civil remedies.

The DOJ's memorandum announcing the new division also underscores a deliberate effort to narrow the traditional gaps between investigative agencies, prosecutors, and civil enforcement components. The designation of [National Fraud Enforcement Division](#) liaisons, the detailing of prosecutors from every U.S. Attorney's Office, and the explicit direction to leverage both criminal and civil enforcement tools suggest that parallel proceedings will become more common. It is reasonable to expect increased use of civil investigative demands, False Claims Act referrals, forfeiture actions, and coordinated charging decisions. For clients — particularly those operating in heavily regulated industries or engaged with federal benefit programs — early internal assessment and privilege-protected compliance reviews will be critical in anticipating exposure across multiple fronts.

Of particular note is the DOJ's emphasis on systems, processes, and "state-of-the-art tools" designed to efficiently identify fraud against taxpayer-funded programs. While the memorandum does not expressly use the term "artificial intelligence," it aligns with the DOJ's broader trajectory toward advanced data analytics, machine learning, and technology-driven fraud detection. The planned National Fraud Detection Center, coupled with expanded analyst, forensic accounting, and FBI resources, suggests increased reliance on automated data matching, anomaly detection, network analysis, and cross-agency data aggregation. This could mean that investigations may increasingly originate from algorithmic red flags rather than whistleblowers or traditional audits — raising novel questions about data accuracy, model bias, explainability, and discovery obligations related to AI-assisted enforcement.

It is important to also take note of the memorandum's forward-looking mandate to evaluate and potentially strengthen laws, regulations, and penalties related to fraud. This signals not only tougher enforcement but also possible statutory or regulatory changes that could lower materiality thresholds, expand intent theories, or enhance penalties. It is reasonable to anticipate heightened False Claims Act scrutiny urged by data-driven referrals, while on the criminal side, you may see an expansion in complex, document-heavy prosecutions supported by forensic technology. In this environment, effective defense will increasingly require fluency not only in substantive fraud law, but also in data governance, technology systems, and the investigative methodologies that underpin modern DOJ cases.

Ultimately, the creation of the National Fraud Enforcement Division reflects a DOJ that is more unified, technologically sophisticated, and proactive in combating fraud. Its memorandum is both a warning and a roadmap: Enforcement actions may come faster, be better coordinated, and rely heavily on advanced analytics. In response, companies that might find themselves in the crosshairs of the government must adapt by engaging earlier, understanding the technological underpinnings of government investigations, and strengthening compliance and data integrity before enforcement interest turns into litigation.

If you have questions about how these DOJ developments may impact your organization or need guidance on responding strategically to government enforcement actions, please contact the authors or any attorney with FBT Gibbons' [White Collar and Investigations](#) practice.

© 2026 FBT Gibbons LLP. May be considered attorney advertising in some jurisdictions.