CADWALADER

The False Claims Act Takes Center Stage

January 5, 2026

By Martin Weinstein
Partner

By Gina Castellano
Partner

By Laura Perkins
Partner

2025 saw heightened enforcement of the FCA in both the healthcare and government contracting industries. In April, the DOJ, with assistance from the Department of Health and Human Services (HHS), reached a $300 million FCA settlement with **Walgreens** resolving allegations that the pharmacy sought payment from federal payors for illegal opioid prescriptions, as well as a $202 million FCA settlement with **Gilead Sciences** resolving allegations that it paid kickbacks, including speaking fees, lavish dinner programs, and all-expense-paid trips, to induce doctors to prescribe Gilead's HIV drugs, thereby causing false claims for the drugs to be filed. In July, the DOJ and HHS **announced** the relaunch of a DOJ-HHS FCA Working Group, initially formed in 2020 under the first Trump administration. The relaunch followed the DOJ's announcement that it was partnering with other agencies as part of the **National Health Care Fraud Takedown** to "bring together experts from the Department's Criminal Division, Fraud Section, Health Care Fraud Unit Data Analytics Team; HHS-OIG; FBI; and other agencies to leverage cloud computing, artificial intelligence, and advanced analytics to identify emerging health care fraud schemes."

Enforcement in the FCA space was particularly active in 2025 with respect to cybersecurity requirements. The DOJ has secured settlements with four defense contractors (**MORSECORP, Inc.**, **Raytheon**, **Aero Turbine, Inc.**, and most recently, **Swiss Automation Inc.**) for failing to comply with cybersecurity requirements in federal contracts. And, as we detailed **previously** in August, the DOJ used the FCA for the first time to enforce cybersecurity standards against medical device company **Illumina**, demonstrating an expanded usage of the FCA. Notably, the DOJ has pursued these FCA actions where cybersecurity standards were not met regardless of whether any actual cybersecurity breaches occurred.

Moving into 2026, we expect to see steady enforcement of the FCA in the healthcare and defense contracting industries alongside use of the FCA to target new enforcement priority areas. For example, we anticipate that the DOJ will continue to use the FCA to pursue trade and customs fraud as it did in 2025. In July, the DOJ's Civil Division reached a $6.8 million settlement with subsidiaries of **MGI**, resolving potential civil liability under the FCA for failure to pay customs duties on plastic imported from China. In August, the DOJ launched a **Trade Fraud Task Force** with the Department of Homeland Security (DHS) to "aggressively pursue enforcement actions against any parties who seek to evade tariffs and other duties, as well as smugglers who seek to import prohibited goods into the American economy." Notably, the announcement invited "whistleblowers to utilize the *qui tam* provisions of the False Claims Act to alert the government to credible allegations of fraud." In December, the DOJ's Civil Division reached a $54.4 million settlement with **Ceratizit**, resolving allegations that Ceratizit violated the FCA by knowingly misrepresenting the country of origin on Chinese-manufactured products to avoid paying tariffs. And, in line with the Civil Division's **Enforcement Priorities**, we may see the DOJ utilize the FCA with respect to illegal discrimination. Indeed, recent **reporting** indicates that the DOJ has issued Civil Investigative Demands to companies across a variety of industries seeking information relating to the employers' diversity, equity, and inclusion programs.

As enforcement of the FCA continues to expand, companies interacting with the government and federally funded programs should continuously monitor their compliance programs. A corporate culture that demonstrates an emphasis on compliance—specifically, highlighting and demonstrating ethical conduct and timely responding and remediating employee concerns—will help to drive potential whistleblowers through internal channels.