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

DOJ'S False Claims Act Based Civil Cyber-Fraud Initiative in 2024

Article By:

Vipal Patel

Karen R. Harbaugh

Kevin Kumar

The start of a new year presents an opportune time to reflect on the past. We have been tracking and reporting on the U.S. Department of Justice ("DOJ")'s Civil Cyber-Fraud Initiative ("CCF Initiative"), which former U.S. Deputy Attorney General Lisa O. Monaco announced in October 2021. The CCF Initiative employs the powerful False Claims Act ("FCA") in an effort to "hold accountable entities or individuals that put U.S. information or systems at risk by (1) knowingly providing deficient cybersecurity products or services, (2) knowingly misrepresenting their cybersecurity practices or protocols or (3) knowingly violating obligations to monitor and report cybersecurity incidents and breaches."

We previously offered insight into the first two FCA enforcement actions brought under this initiative, then a third, and a fourth. 2024 brought even more.

Towards the end of 2024, on October 22, 2024, DOJ announced an FCA settlement with a major public university relating to its alleged failure to comply with cybersecurity requirements for more than a dozen Department of Defense ("DOD") and National Aeronautics and Space Administration ("NASA") contracts and subcontracts. The university agreed to pay $1.25M to resolve allegations that it violated the FCA by failing to comply with cybersecurity requirements in fifteen contracts or subcontracts involving the DOD or NASA. The settlement resolves allegations brought by a chief information officer for the university's Applied Research Laboratory in October 2022 under the FCA's *qui tam* provisions.

The covered conduct includes allegations that the university failed to implement certain cybersecurity controls that were contractually required, and did not adequately develop and implement plans of action to correct deficiencies it identified. Specifically, the allegation was that the university did not implement certain National Institute of Standards and Technology requirements. There were no allegations that a third party ever breached any secured data within the university's custody; the university's alleged noncompliance alone was sufficient to fall in DOJ's crosshairs.

Just a week prior, on October 15, 2024, a government services contractor agreed to pay $306,722 and waive $877,578 in potentially reimbursable remediation costs to settle allegations that it failed to properly protect personally identifiable information and personal health information of Medicare beneficiaries, resulting in a data breach. Despite the contractor promptly notifying Centers for Medicare and Medicaid Services ("CMS") and cooperating with DOJ investigation, DOJ still pursued a FCA violation. The allegations stemmed from a shift to the electronic handling of "certain Medicare Support services" during the COVID-19 pandemic that the contractor provided to CMS between March 2021 and October 2022. Under its agreement with the CMS, the contractor was required to adhere to the Department of Health and Human Services ("HHS")'s cybersecurity requirements. However, a *subcontractor*, whose servers were used to carry out the electronic task, was allegedly not in compliance with HHS' cybersecurity requirements. Specifically, the subcontractor allegedly took screenshots from CMS systems that contained personally identifiable information and stored the screenshots without encryption, violating HHS' cybersecurity requirements. Notably, per DOJ, "[t]he subcontractor's server was breached by a third party in October 2022 and the unencrypted screenshots were allegedly compromised during that breach."

These two FCA settlements under the CCF Initiative are only the latest reverberations of DOJ's increased scrutiny on cybersecurity compliance to combat emerging cyber threats. There were others in 2024, including these three that were highlighted in DOJ's annual recap of its FCA enforcement endeavors:

- **May 1, 2024**: a staffing company agreed to pay $2.7M to resolve allegations that it violated the FCA by failing to implement adequate cybersecurity measures to protect health information obtained during COVID-19 contact tracing.
- **June 17, 2024**: two consulting companies agreed to pay a combined $11.3M to resolve allegations that they violated the FCA by failing to meet cybersecurity requirements in contracts intended to ensure a secure environment for low-income New Yorkers to apply online for federal rental assistance during the COVID-19 pandemic.
- **August 22, 2024**: DOJ filed an Amended Complaint against another major public university, alleging that it failed to meet certain cybersecurity requirements in its performance of DOD contracts. The university has moved to dismiss, and the motion is pending. The university's argument is that the pertinent contract was for fundamental research and therefore not subject to DOD cybersecurity rules. DOJ contested the notion in its opposition and, as to materiality, took the position that "common sense alone supports the materiality of the cybersecurity requirements Defendants allegedly breached." The university's reply primarily dealt with the materials the Court could consider to resolve the issue. The matter is pending.

The enforcement actions brought in 2024 show the breadth of the CCF Initiative. That enforcement actions have been brought even where *no breach occurred* broadens the scope even more. What 2025 will bring, particularly in light of the administration change (and certain percolating constitutional challenges to components of the FCA), remains to be seen.

Whether the CCF Initiative continues in current form, name, or fervor, it nonetheless underscores the importance for contractors, subcontractors, grantees, and other forms of funding that have agreements with the government to pay close attention to the cybersecurity requirements of such agreements. If have not done so already, companies should consider engaging with counsel in concert with knowledgeable information technology professional (either external or internal) to:

1. understand their cybersecurity obligations on existing and future U.S. government contracts, subcontracts, grants and other forms of funding,

2. train employees,
3. implement information security controls such as access and network restrictions,
4. invest in and ensure regular compliance with upgrades, patches, and maintenance,
5. devise incident response plans and ransom strategies, and
6. operationalize internal whistleblowing.

And should a cyber incident occur, entities need to consider any Federal Acquisition Regulation ("FAR") and/or agency FAR supplemental clause disclosure requirements in addition to any other Federal and state cyber incident reporting requirements applicable to the incident, e.g., HIPAA.

© Copyright 2025 Squire Patton Boggs (US) LLP

National Law Review, Volume XV, Number 59

Source URL:https://natlawreview.com/article/dojs-false-claims-act-based-civil-cyber-fraud-initiative-2024