Articles + Publications | April 21, 2022

Federal Contractors on Notice After DOJ Announces First Civil Cyber Fraud Initiative Settlement

WRITTEN BY

Ronald I. Raether Jr. | Ashley L. Taylor, Jr. | Daniel Waltz | Hilary S. Cairnie | John Sample

On February 28, the U.S. Department of Justice (DOJ) agreed to a $930,000 settlement with Comprehensive Health Services (CHS) to resolve False Claims Act allegations. The resolution represents the department's first settlement under the False Claims Act since instituting its Civil Cyber Fraud Initiative in October 2021.[1] This is a watershed moment in the department's approach to cybersecurity that highlights its renewed focus and commitment to holding vendors that do business with the federal government accountable for meeting federal cybersecurity requirements.

Civil Cyber Fraud Initiative

In October 2021, the department announced the launch of its Civil Cyber Fraud Initiative, which seeks to combine the department's expertise in civil fraud enforcement, government procurement, and cybersecurity to combat new and emerging cyber threats to the security of sensitive information and critical systems. The department touted this initiative as a direct response to the lack of disclosure and reporting by government contractors when faced with breaches. "For too long, companies have chosen silence under the mistaken belief that it is less risky to hide a breach than to bring it forward and to report it," said Deputy Attorney General Monaco. Specifically, the initiative seeks to hold government contractors accountable when they fail to follow the federal government's cybersecurity requirements.

The initiative targets companies and individuals that place U.S. information or systems at risk by knowingly providing deficient cybersecurity products or services, knowingly misrepresenting their cybersecurity practices or protocols, or knowingly violating obligations to monitor and report cybersecurity incidents and breaches.

The initiative further employs the False Claims Act as an avenue to pursue cybersecurity-related fraud by government contractors and grant recipients. Historically, the False Claims Act has operated as the government's primary civil tool to redress false claims for federal funds and property involving government programs and operations. As such, only those companies that receive federal assets are subject to scrutiny under the False Claims Act with this initiative.

Settlement Emphasizes Contractors Must Comply With Cybersecurity Requirements in Federal Contracts

CHS, a provider of global medical services, contracted to provide medical support services at government facilities in Iraq and Afghanistan. Under one of those contracts, CHS submitted claims to the State Department for the cost of a secure electronic medical record (EMR) system to store all patient medical records, including the confidential

©2025 Troutman Pepper Locke

identifying information of U.S. service members, diplomats, officials, and contractors working and receiving medical care in Iraq. The United States alleged that CHS violated the False Claims Act by falsely representing that it complied with contract requirements relating to the provision of medical services at State Department and Air Force facilities in Iraq and Afghanistan.

Specifically, the United States asserted that between 2012 and 2019, CHS failed to disclose that it had not consistently stored patients' medical records on a secure EMR system, as required under its contract. The department explained that "when CHS staff scanned medical records for the EMR system, CHS staff saved and left scanned copies of some records on an internal network drive, which was accessible to non-clinical staff. Even after staff raised concerns about the privacy of protected medical information, CHS did not take adequate steps to store the information exclusively on the EMR system." Instead, CHS allegedly charged the State Department almost $500,000 for the EMR system, but it failed to disclose that it also stored medical records on the internal network drive where nonclinical staff would have access. In essence, the United States asserted that it bargained and paid for secure storage of medical records but did not receive the benefit of that bargain in light of CHS's *knowing* misrepresentations that medical records were stored only in secure locations.

As expressed by Principal Deputy Assistant Attorney General Brian M. Boynton, head of the DOJ's Civil Division, "[T]his settlement demonstrates the department's commitment to use its civil enforcement tools to pursue government contractors that fail to follow required cybersecurity standards, particularly when they put confidential medical records at risk."

The civil settlement includes the resolution of two actions brought under the *qui tam* or whistleblower provisions of the False Claims Act against CHS. Under the *qui tam* provisions of the False Claims Act, a private party can file an action on behalf of the United States and receive a portion of the settlement if the government takes over the case and reaches a monetary agreement with the defendant. The *qui tam* cases are captioned *United States ex rel. Lawler v. Comprehensive Health Servs., Inc. et al*., Case No. 20-cv-698 (E.D.N.Y.) and *United States ex rel. Watkins et al. v. CHS Middle East, LLC*, Case No. 17-cv-4319 (E.D.N.Y.).

Takeaways

The investigation and subsequent settlement of this case underscores the department's renewed focus on combatting cyber fraud, as well as its willingness to utilize any legal measure available to it. It is clear that the DOJ will target companies that *knowingly* provide products and services that are noncompliant with contractual cybersecurity requirements. Accordingly, it is vital that companies carefully evaluate compliance mechanisms and document cybersecurity compliance efforts with specific contractual requirements in mind. As a best practice, companies that contract with the federal government should consider the following best practices:

- Understand up front that the frequently imposed cybersecurity requirements embodied at FAR 52.204-21and DFARS 252.204-7012 also incorporate cybersecurity standards established by, for example, the National Institute for Standards and Testing (NIST). The most commonly adopted standards are those at NIST SP 800-171 (addressing a total of 110 distinct cybersecurity functions and features). Moreover, many federal agencies include in their contracts additional cybersecurity requirements in the form of tailored contract clauses developed to address their unique mission requirements (NASA, VA, DHS, DHHS, DOE, NIS, to name a few).

- Ensure that cybersecurity and privacy policies are current and compliant with the terms of the contract.
- Implement a program to update security policies on a cadence that allows for changes consistent with federal guidance and the terms of contract renewals.
- Employ third parties to test the policies and conduct gap analyses to ensure all necessary security requirements are covered in both written policy and in practice. If you are a DOD contractor, you are most likely subject to the standards enumerated in NIST SP 800-171, which require, among other things, that you perform a gap analysis and prepare objectives and milestones (POAM). Over time, and with effort and investment, the stated objectives and milestones will be achieved and full compliance accomplished.
- Develop processes to test and validate material representations and certifications made to the government regarding bidding, negotiating, and performing awarded contracts. Document those processes and ensure that objective evidence supporting such representations and certifications is preserved.
- Ensure that the company and its employees are knowledgeable about reporting obligations regarding changes in cybersecurity risk, cyber incidents, data breach, and other material elements relating to federal contract and grants. While an inadvertent failure to comply with the terms of a federal award is not ideal, failure to adequately and properly disclose such a failure will be significantly worse for the company.
- Take seriously internal reports, complaints, and suggestions from employees expressing their observations and concerns about the company's compliance or perceived noncompliance with contractual cybersecurity obligations.[2]

Be sure to seek legal advice from attorneys with the requisite expertise to both identify and manage cybersecurity requirements and appropriately address any compliance gaps of the company.

Troutman Pepper has considerable expertise and knowledge at the intersection of law and technology and consistently monitors this space for developments to advise clients in this rapidly evolving landscape. Troutman Pepper attorneys also possess the requisite experience and expertise to provide sophisticated and customized legal solutions to companies challenged with disputes centering on the False Claims Act.

---

[1] While this is the DOJ's first settlement using the FCA under the Civil Cyber Fraud Initiative, it is not the first time the FCA has been used to allege cyber fraud with government contracting. In *United States ex rel. Markus v. Aerojet RocketDyne Holdings, Inc.*, the DOJ filed a statement of interest in opposition to Aerojet's motion for summary judgment, arguing that it contracted with Aerojet not only to build rocket engines, but also to securely store government data on systems that met certain cybersecurity requirements. The Eastern District of California denied Aerojet's motion for summary judgment. The DOJ did not intervene in the *qui tam* action.

[2] In the *Aerojet* case, for years, management allegedly ignored complaints from one or more employees about intentional noncompliance and false certifications.

RELATED INDUSTRIES + PRACTICES

- Privacy + Cyber
- State Attorneys General