ALERT MEMORANDUM

Recent Developments Shed Light on the Justice Department's Civil Cyber-Fraud Initiative

March 14, 2022

In October 2021, the U.S. Department of Justice announced the launch of its new Civil Cyber-Fraud Initiative, which aims to hold government contractors and grant recipients accountable for cyber-related fraud under the False Claims Act. Two recent developments provide insight into how the Justice Department will pursue cases under this new initiative, and reveal the broad conception of cyber fraud the Department is advocating in such cases.

- *Comprehensive Health Services LLC*: On March 8, 2022, the Justice Department announced its first settlement under the Civil Cyber-Fraud Initiative. Comprehensive Health Services, LLC, a global medical services provider, agreed to pay $930,000 to resolve allegations that it falsely represented to the federal government that it had consistently stored patient records on a secure electronic system. The Justice Department intervened in the matter, which was brought originally by private whistleblowers, despite the fact that no breach of data was alleged to have occurred.
- *Aerojet RocketDyne Holdings, Inc.*: On February 1, 2022, a federal court in the Eastern District of California mostly denied summary judgment to Aerojet Rocketdyne Holdings Inc., a defense and aerospace company that is alleged to have falsely represented its compliance with cybersecurity standards for government contractors. The Justice Department filed a Statement of Interest that was largely adopted by the district court to reject Aerojet's arguments that its alleged non-compliance was immaterial and did not harm the government.

If you have any questions concerning this memorandum, please reach out to your regular firm contact or the following authors.

Bay Area

Jennifer Kennedy Park
+1 212 225 2357
jkpark@cgsh.com

Ye Eun Charlotte Chun
+1 650 815 4111
chchun@cgsh.com

New York

Anthony M. Shults
+1 212 225 2693
ashults@cgsh.com

The Civil Cyber-Fraud Initiative

On October 6, 2021, Deputy Attorney General Lisa O. Monaco announced the launch of the Justice Department's Civil Cyber-Fraud Initiative, which will utilize the False Claims Act ("FCA") to pursue cyber-fraud committed by government contractors and grant recipients. The initiative is led by the Civil Division's Commercial Litigation Branch, and is focused on holding contractors and grant recipients accountable for knowingly:

(1) providing deficient cybersecurity products or services to the government;

(2) misrepresenting their cybersecurity practices or protocols; or

(3) violating obligations to monitor and report cybersecurity incidents and breaches.[1]

The FCA imposes liability for knowingly presenting materially false or fraudulent claims for payment from the federal government, and for knowingly making false statements material to a false or fraudulent claim.[2] The statute serves as the federal government's primary civil tool to obtain redress for false claims for government funds.[3]

The FCA also allows private citizens to file suits on the government's behalf – known as *qui tam* actions. The government can choose to intervene in such actions and take over the conduct of the case. Individuals who bring *qui tam* suits are referred to as "relators" and may receive a portion of any recovery by the government.

The Aerojet Case

Aerojet Rocketdyne is a defense and aerospace company that contracts with federal agencies, including the Department of Defense and NASA. Former employee Brian Markus brought a *qui tam* suit alleging that Aerojet committed promissory fraud and made false certifications regarding its cybersecurity compliance as required by the Federal Acquisition Regulations ("FAR") and other supplementary agency-specific regulations applicable to government contractors.

Justice Department's Statement of Interest

In 2018, the Justice Department declined to intervene as a party in the action. However, on October 20, 2021 – two weeks after the launch of the Civil Cyber-Fraud Initiative – the Justice Department filed a Statement of Interest responding to arguments raised in Aerojet's motion for summary judgment.

Primarily, the Justice Department disputed Aerojet's position that its non-compliance with applicable cybersecurity requirements had no effect on the government's contracting decisions. Relying on Ninth Circuit precedent,[4] the Department maintained that an agency's failure to end a contractual relationship after learning of a *qui tam* suit does not preclude a finding of promissory fraud.[5]

Separately, the Justice Department argued that non-compliance with cybersecurity requirements can be material even when the federal government

[1] Deputy Attorney General Lisa O. Monaco Announces New Civil Cyber-Fraud Initiative, U.S. Dep't of Justice (Oct. 6, 2021), https://www.justice.gov/opa/pr/deputy-attorney-general-lisa-o-monaco-announces-new-civil-cyber-fraud-initiative.

[2] 31 U.S.C.A. § 3729 (2022).

[3] Indeed, the Justice Department obtained more than $5.6 billion in settlements and judgments from FCA cases in 2021 alone. The False Claims Act, U.S. Dep't of Justice, https://www.justice.gov/civil/false-claims-act (last updated Feb. 2, 2022).

[4] *United States ex rel. Campie v. Gilead Scis., Inc.*, 862 F.3d 890, 904 (9th Cir. 2017).

[5] United States' Statement of Interest in Connection with Defendants' Summary Judgment Motion at 3, *United States ex rel. Markus v. Aerojet RocketDyne Holdings, Inc.*, No. 2:15-cv-02245 (E.D. Cal. Oct. 20, 2021), Docket No. 135 (hereinafter "Statement of Interest").

makes payment with partial knowledge of a contractor's non-compliance generally.[6]

Lastly, the Justice Department maintained that actual damages could exist even if a contractor delivered functional products and, importantly, even if there was no data loss or other cybersecurity breach as a result of the company's cyber non-compliance.

The Court's Summary Judgment Decision

As noted above, the district court largely adopted the Justice Department's arguments. The Court observed that compliance with the cybersecurity standards "was an express term of the contracts," and "[i]t may be reasonably inferred that compliance was significant to the government because without complete knowledge about compliance . . . the government cannot adequately protect its information."[7] The Court also held that there were triable issues of fact as to whether Aerojet knowingly misrepresented its compliance to the government and whether Aerojet's alleged fraud caused the government to continue its contractual relationship with the company. The claim for promissory fraud can thus proceed to trial.

The Comprehensive Health Services Settlement

Comprehensive Health Services ("CHS") is a global medical services provider that contracted with the U.S. State Department and Air Force to provide medical support services at government-run facilities in Iraq and Afghanistan. Under one of its contracts, CHS submitted claims to the State Department for the cost of a secure electronic medical record ("EMR") system to store patients' medical records, including confidential identifying information of U.S. government employees.[8]

Relators alleged that between 2012 and 2019, CHS failed to consistently store these medical records on the secure EMR system, despite having invoiced the government for its use. Instead, CHS employees had saved and left scanned copies of these records on an internal network drive, which was accessible to non-clinical staff. [9]

In February 2022, the United States moved to intervene in the matter for the purposes of settlement. To resolve the allegations, CHS agreed to pay $930,000 to the government.

Takeaways

These recent developments provide the first key insights into the Justice Department's Civil Cyber-Fraud Initiative, which will likely pick up steam throughout 2022.

- The positions taken by the Justice Department reflect an aggressive approach to holding contractors accountable for cybersecurity practices that fall short of contractual obligations, even in the absence of a significant data breach or other cyber incident. The government is likely to continue to maintain that cyber compliance represents a material component of its contractual relationships with government contractors and grant recipients.

[6] Statement of Interest at 6.
[7] Memorandum and Order re: Cross-Motions for Summary Judgment at 16, *United States ex rel. Markus v. Aerojet RocketDyne Holdings, Inc.*, No. 2:15-cv-02245 (E.D. Cal. Feb. 1, 2022), Docket No. 155 (hereinafter "Order").
[8] Contractor Pays $930,000 to Settle False Claims Act Allegations Relating to Medical Services Contracts at State Department and Air Force Facilities in Iraq and Afghanistan, U.S. Dep't of Justice (Mar. 8, 2022), https://www.justice.gov/usao-edny/pr/contractor-pays-930000-settle-false-claims-act-allegations-relating-medical-services.
[9] *Id.*

- Companies that contract with the federal government must take seriously their obligations to comply with cybersecurity requirements set out in their contracts and in applicable regulations like FAR. Additionally, such companies should ensure that they have cyber-related policies and controls in place and that they fully and accurately disclose their compliance records with their contractual counterparts.

…

CLEARY GOTTLIEB