GT GreenbergTraurig

Alert | Government Contractor Cybersecurity

May 2022

DOJ's Cyber-Fraud Initiative: Increased False Claims Act Scrutiny of Contractor Cybersecurity Compliance

This GT Alert covers the following:

- Department of Justice Cyber Fraud Initiative raises stakes for contractor and grant recipient non-compliance with cybersecurity requirements
- Two recent settlements highlight increased False Claims Act scrutiny and potentially costly *qui tam* actions that can result from non-compliance with federal cybersecurity requirements

Accuracy in contractor proposal representations and cybersecurity compliance remains pressing, as demonstrated by an April 2021 settlement under the False Claims Act (FCA). In a previous alert, we noted that contractor representations of cybersecurity compliance/capabilities represent a fertile ground for bid protests. In this GT Alert, we highlight how the Department of Justice (DOJ) Cyber Fraud Initiative and *qui tam* actions under the FCA represent significant enforcement mechanisms that raise the stakes for non-compliance with evolving cybersecurity requirements applicable to contractors and grant recipients.

On Oct. 6, 2021, DOJ announced its Civil Cyber-Fraud Initiative. This initiative uses the FCA to hold contractors and grantees accountable for knowingly furnishing deficient cybersecurity products/services, misrepresenting cybersecurity practices, or knowingly violating obligations to report cybersecurity incidents. DOJ, acting on behalf of the United States, entered into its first settlement to resolve two False Claims Act cases under the Civil Cyber-Fraud Initiative. *United States ex rel. Watkins et al. v. CHS Middle*

East, LLC, No. 17-cv-4319 (E.D.N.Y. Feb. 28, 2022); *United States ex rel. Lawler v. Comprehensive Health Servs., Inc. et al.*, No. 20-cv-698 (E.D.N.Y. Feb. 28, 2022).

Comprehensive Health Services LLC (CHS), a global medical services provider, contracted to service government-run facilities in Iraq and Afghanistan. Under one such contract with the State Department, CHS submitted claims for the cost of a secure electronic medical record (EMR) system to store patient medical records, including the confidential identifying information of U.S. service members, diplomats, officials, and contractors working and receiving medical care in Iraq. Among the allegations, spanning the performance period from 2011 through 2021, the United States alleged that CHS had not securely stored patient medical records, left scanned copies of records on an internal network drive (accessible to non-clinical staff presumably without a need to know), and failed to take adequate steps to remedy raised concerns from staff about the safe storage of such information. While the settlement is not an admission of liability by the contractor, the parties agreed to settle for $930,000 in the interest of avoiding the expense of litigation.

Although the *CHS* case represented the first settlement under DOJ's Civil Cyber-Fraud Initiative, it is not the first time a contractor has been hit with FCA claims based on non-compliance with cybersecurity requirements. In a case filed in 2015, *United States ex rel. Markus v. Aerojet Rocketdyne Holdings, Inc.*, a former employee alleged that his previous employer, Aerojet Rocketdyne Holdings, Inc. (ARH), violated the FCA by failing to safeguard unclassified controlled technical information from cybersecurity threats as required. The relator claimed that ARH knew its computer systems failed to meet the cybersecurity requirements of applicable agency regulations and that ARH received its contract award based on misleading statements by not fully disclosing the extent of its noncompliance. In a blow to the defense, the district judge ruled in a February 2022 decision that genuine issues of material fact existed as to whether the defendant federal contractor had made misrepresentations to the government concerning its cybersecurity capabilities and so denied ARH's motion for summary judgement. On April 27, 2022, ARH agreed to pay roughly $9 million to settle the relator's False Claims Act claims.

Key Takeaways

The recent settlements of FCA claims in *United States v. Comprehensive Health Services, Inc.* and *United States v. Aerojet Rocketdyne Holdings, Inc.* are reminders that misrepresentations regarding cybersecurity compliance may give rise to *qui tam* suits and liability under the FCA. DOJ's Civil Cyber-Fraud Initiative may result in an increased number of actions alleging noncompliance with evolving contractor cybersecurity requirements.

Authors

This GT Alert was prepared by:

- Scott A. Schipma | +1 202.331.3141 | schipmas@gtlaw.com
- Aaron M. Levin | +1 202.533.2316 | levinaa@gtlaw.com