PUBLICATION

Cybersecurity: A Whistleblower's Paradise

Authors: Alisa L. Chestler
April 14, 2022

Cyber whistleblowing is the newest and hottest area of exposure for organizations. All government contractors and grant recipients must develop an understanding of the use of the False Claims Act (FCA) to address cybersecurity concerns. In the last month, there have been several significant cases and actions from the Biden Administration that deserve close attention.

Rapidly evolving technological advances, new forms of attacks and lack of government cybersecurity enforcement have created an atmosphere in which potential non-compliance or misstatements could create opportunities that whistleblowers will soon feast upon.

The United States Department of Justice's (DOJ) Civil Cyber-Fraud Initiative (the Initiative) was first announced in October 2021. The Initiative paved the way for use of the FCA to address government contractors and grant recipients that submit false claims misrepresenting compliance with cybersecurity standards related to information technology, software, cloud-based storage, and other related services. Generally, the FCA provides a civil remedy when a party knowingly presents or causes a false claim to the government for payment. Any individual or organization who submits or causes to be submitted claims for payment to the government is subject to potential FCA liability. One way a claim can be false is when an organization attests to or certifies compliance with terms of the government contract or the regulatory requirements of the service or product, but the organization is actually not in compliance with those requirements.

Specifically, the DOJ indicated cybersecurity non-compliance will be ripe for an FCA claim when the organization:

- knowingly provides deficient cybersecurity products or services;
- knowingly mispresents their cybersecurity practices and protocols; or
- knowingly violates obligations to monitor and report cybersecurity incidents and breaches.

The FCA includes significant enticement for whistleblowers under its *qui tam* provisions because it allows whistleblowers to bring claims on behalf of the government and get a 15 percent to 30 percent cut of any civil recovery that comes from settlement, judgment, or verdict.

Comprehensive Health Services, LLC (CHS) Settles FCA Allegations for $930,000

On March 8, 2022, the DOJ resolved its first False Claims Act case under the Civil Cyber-Fraud Initiative. The DOJ alleged that CHS violated the FCA when it falsely attested to compliance with government contracts relating to the provision of medical services at government facilities in Iraq and Afghanistan.

CHS is a global provider of medical services. As part of its government contract, CHS submitted claims and was reimbursed for implementation of a secure electronic medical record (EMR) system. The system would be used to store patient's medical records and consequentially the information would include confidential identifying information of United States service members, diplomats, officials, and government contractors receiving care at the facilities. The DOJ alleged that CHS failed to disclose it had not consistently stored

records on the EMR and staff had saved some records on the entity's internal network drive, which did not limit access to only clinical staff. The DOJ further alleged that, after staff raised concerns about the unsecure storage of protected health information, CHS did not take appropriate steps to remediate the issue.

CHS's $930,000 civil settlement to resolve the DOJ's allegations includes the resolution of two separate actions brought by whistleblowers under the FCA's *qui tam* provisions. In the Department of Justice's press release, Special Agent in Charge Elizabeth Kaminsky of the U.S. Department of State Office of Inspector General commented that the Agency's hope was "that this outcome will send a clear message that cutting corners on State Department contracts has significant consequences."

Aerojet Rocketdyne Faces FCA Whistleblower Case

The Aerojet Rocketdyne (Aerojet) case originally filed in 2015 came when the whistleblower, who worked as the company's Senior Director of Cyber Security, Compliance & Controls, grew frustrated and concerned regarding Aerojet's information security program and resources. The whistleblower alleged in his second amended complaint that:

- The provisions in the Department of Defense and NASA contracts required that Aerojet meet certain cybersecurity standards and adhere to certain cybersecurity regulations.
- Aerojet entered into the contracts knowing that they did not meet the minimum standards and they further misled the government by concealing their non-compliance.
- Although the company reported computer system breaches in 2013 and 2014, Aerojet concealed that its computer system was non-compliant with cybersecurity requirements.
- The whistleblower attempted to notify the board of the non-compliance, but that attempt was allegedly quashed by the Aerojet president.
- Aerojet management was allegedly aware that they were out of compliance with the cybersecurity standards and regulations.

The government declined to intervene in the case in 2018 but changed course in October 2021 and filed a statement of interest in support of the case. The jury trial is set to begin April 26, 2022, in the U.S. District Court for the Eastern District of California.

These examples of FCA enforcement should serve as a wake-up call for organizations that non-compliance with cybersecurity standards, contractual requirements, and applicable cybersecurity regulations will no longer be tolerated. It is time to mitigate the risk of whistleblower actions by ensuring the organization has an internal mechanism for reporting potential cybersecurity compliance. Furthermore, it is essential to respond to any complaints with meaningful steps to achieve compliance. If an organization has potential FCA exposure related to cybersecurity, it is imperative to consult with outside counsel to determine how to best address that exposure.

For more information contact Alisa L. Chestler, CIPP/US or your Baker Donelson Health Law or Data Protection, Privacy and Cybersecurity attorney.