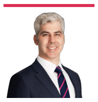
New Cybersecurity Enforcement Through DOJ's Civil Cyber-Fraud Initiative and the False Claims Act

WHITE COLLAR CRIME & GOVERNMENT INVESTIGATIONS | CYBERSECURITY AND PRIVACY | GOVERNMENT CONTRACTS | OCTOBER 12, 2021


Michael L. Yaeger


Natalie A. Napierala


Katelyn M. Sandoval

On October 6, 2021, the Department of Justice opened up a new front in cybersecurity compliance when it announced a Civil Cyber-Fraud Initiative using the False Claims Act and other civil enforcement tools against government contractors and grant recipients.

This raises the specter not just of DOJ enforcement, but more numerous claims by private actors — specifically, whistleblowers or qui tam relators seeking a share of the government's recovery. For example, in *United States ex rel. Markus v. Aerojet Rocketdyne Holdings Inc.*, the relator — a former employee of the defendant — brought two claims of fraud under the False Claims Act. The relator alleged that the "defendants fraudulently entered into contracts with the federal government despite knowing that they did not meet the minimum [cybersecurity] standards required to be awarded a government contract." The court declined to dismiss the False Claims Act claims, finding that the relator had "plausibly pled that defendants' alleged failure to fully disclose its noncompliance [with relevant DOD and NASA regulations] was material to the government's decision to enter into and pay on the relevant contracts." And the potential costs in a case that might stem from the initiative are significant, as the False Claims Act also allows for triple damages.

The DOJ's Fraud Section plans to target government contractors and grant recipients who (1) knowingly provide deficient cybersecurity products or services; (2) knowingly misrepresent their cybersecurity practices or protocols; or (3) knowingly violate obligations to monitor and report cybersecurity incidents and breaches — in other words, bad cybersecurity, misrepresentations about cybersecurity, and failure to report as required by statute, regulation, or contract.

According to the government, the Civil Cyber-Fraud Initiative was formed in direct response to the attitude of many companies that "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." Accordingly, the DOJ plans to use its "civil enforcement tools" to identify government contractors who "fail to follow required cybersecurity standards."

The civil initiative does not preclude parallel criminal enforcement actions. For example, 18 U.S.C. § 287 criminalizes the making of false, fictitious, or fraudulent claims upon the United States or conspiring to do so. It is not uncommon for those U.S. attorney's offices that intervene in False Claims Act cases to assign criminal AUSAs to parallel investigations, so contractors and grant recipients who face a False Claims Act case or investigation should be aware of the possibility as they engage with the government.

Takeaways

- Review your cybersecurity practices and protocols, including related regulations and your government contracts, to make sure your practices comply with federal law.
    - For example, FAR 52.204-21, Basic Safeguarding of Covered Contractor Information Systems, requires contractors to use certain "basic" security controls, such as limiting access, authenticating users, and identifying system flaws in a "timely manner."
- Review your obligations under the False Claims Act and its state law equivalents.
- If you are faced with a civil False Claims Act case, be aware of the possibility that there may be a parallel criminal action.