DOJ "Civil Cyber-Fraud Initiative" Will Use the False Claims Act to Target Government Contractors and Grant Recipients

Litigation Alert
10.11.2021

The U.S. Department of Justice (DOJ) announced on October 6, 2021 the launch of a "Civil Cyber-Fraud Initiative." Led by the Civil Division's Commercial Litigation Branch (Fraud Section), DOJ will use the False Claims Act (FCA) to target government contractors and grant recipients who allegedly put U.S. information or systems at risk of cyber-attack.

Under the initiative, DOJ will focus on bringing actions against contractors who allegedly have knowingly:

1. Provided deficient cybersecurity products or services to the United States;
2. Misrepresented their cybersecurity practices; or
3. Failed to monitor and report cyber breaches.

DOJ's stated goals for the initiative include:

- Building broad resiliency against cybersecurity intrusions across the government, the public sector, and key industry partners
- Holding contractors and grantees to their commitments to protect government information and infrastructure
- Supporting government experts' efforts to timely identify, create, and publicize patches for vulnerabilities in commonly used information technology products and services
- Ensuring that companies that follow the rules and invest in meeting cybersecurity requirements are not at a competitive disadvantage
- Reimbursing the government and taxpayers for the losses incurred when companies fail to satisfy their cybersecurity obligations
- Improving overall cybersecurity practices that will benefit the government, private users, and the American public

As part of this initiative, DOJ says it intends to leverage the resources of other federal agencies and subject matter experts from the government procurement and cybersecurity fields — along with all the tools of the FCA, including its whistleblower provisions. The initiative comes on the heels of the May executive order on cybersecurity issued by the Biden administration (discussed here). Recently, cybersecurity-related FCA claims have become more common, as the following cases demonstrate:

- In *United States v. Aerojet Rocketdyne Holdings, Inc* ., 381 F. Supp. 3d 1240 (E.D. Cal. 2019), a former employee of Aerojet brought an FCA claim, alleging the company was falsely certifying that it was in compliance with Department of Defense cybersecurity standards. The court denied Aerojet's motion to dismiss, asserting that the relator's claim sufficiently showed the company's alleged nondisclosure was material to the government's award decision.
- In 2019, Cisco settled an FCA action between the company and the federal and several state governments for $8.6 million. The action resolved a lawsuit originally brought in 2011, *United States ex rel. Glenn v. Cisco Systems, Inc* ., No. 1:11-cv-00400- RJA (W.D.N.Y. July 31, 2019), by a whistleblower who alleged that Cisco knowingly sold video surveillance equipment to the government that was suspectable to cybersecurity breaches.

- In *United States ex rel. Adams v. Dell Computer Corp* ., No. 15-CV-608 (TFH), 2020 WL 5970677 (D.C. Cir. Oct. 8, 2020), a whistleblower alleged that Dell sold computers with undisclosed security vulnerabilities to the government. The Court found the claim did not meet the demanding standards of a false certification theory under the FCA — namely, that the defendant knowingly misrepresented noncompliance and that the compliance was material to the government's decision to pay — neither of which were proven in the case.

DOJ's announcement suggests that these FCA cases are just the tip of the iceberg and that a much larger wave of cyber-focused FCA enforcement may soon be upon us.

We will continue to monitor and report on DOJ's work in connection with the Civil Cyber-Fraud Initiative. In the meantime, if you have any questions about the FCA or any cybersecurity compliance matters, please contact one of the Miller & Chevalier attorneys listed below.

Alex Sarria, asarria@milchev.com, 202-626-5822

Jason Workmaster, jworkmaster@milchev.com, 202-656-5893

Connor Farrell, a law clerk in the government contracts group, contributed to this client alert.