WINSTON & STRAWN LLP

BLOG

DOJ Launches Civil Cyber-Fraud Initiative to Use False Claims Act to Enforce Federal Contractors' Cyber Security Requirements

NOVEMBER 2, 2021

On October 6, 2021, Deputy Attorney General Lisa O. Monaco announced a new Civil Cyber-Fraud Initiative through which the Department of Justice (DOJ) will utilize the False Claims Act (FCA) as a tool to enforce cybersecurity standards required of federal contractors and grant recipients. Specifically, the DOJ will target companies and individuals that allegedly misrepresent their cybersecurity practices or protocols to win a federal contract or grant or that knowingly submit claims to the government for payment while in violation of regulatory or contractual cybersecurity requirements.

The Biden administration has signaled that it views national cybersecurity as an important enforcement priority. In May 2021, President Biden signed an Executive Order on Improving the Nation's Cybersecurity, stating that "the Federal Government must bring to bear the full scope of its authorities and resources to protect and secure its computer systems." That same month, Deputy AG Monaco ordered a comprehensive cyber review "aimed at developing actionable recommendations to enhance and expand the Justice Department's efforts against cyber threats." The Civil Cyber-Fraud Initiative arose from that review.

In light of the FCA's treble-damages provisions and increased penalties of up to $23,607 *per claim*, the Act continues to incentivize private citizens, or relators, to bring *qui tam* (i.e., whistleblower) lawsuits on behalf of the government and collect a hefty relator's share. A classic example of a false claim is where a contractor fraudulently receives payment from the government for goods or services it did not actually provide.

But a contractor also faces potential FCA liability for falsely certifying that it complied with a legal or contractual obligation—even where it provided goods or services in accordance with the contract—if it can be shown that the noncompliance is material to the government's decision whether to pay the claim. The Supreme Court recognized in its landmark *Escobar* decision that false certifications may be express or implied: "the implied false certification theory can be a basis for liability . . . when the defendant submits a claim for payment that makes specific representations about the goods or services provided, but knowingly fails to disclose the defendant's noncompliance with a statutory, regulatory, or contractual requirement."[1] Some courts have specifically found that an alleged false certification of compliance with cybersecurity protocols required to do business with the government may form the basis for FCA liability.[2]

In an October 13, 2021 speech at the Cybersecurity and Infrastructure Security Agency's National Cybersecurity Summit, Brian Boynton, assistant acting attorney general for the DOJ Civil Division, gave the following rationale for using the FCA framework for enforcing cybersecurity requirements against federal contractors:

> Importantly, [the Civil Cyber-Fraud Initiative] will focus on cases where federal agencies are victims. When companies that do business with the government knowingly make misrepresentations about their own cybersecurity practices, or when they fail to abide by cybersecurity requirements in their contracts, grants or licenses, the government does not get what it bargained for. Even more significantly, when false assurances are made to the government, sensitive government information and systems may be put at risk without the government even knowing it.

Boynton described three types of knowing misconduct by federal contractors as "prime candidates" for FCA enforcement under the new initiative:

1. noncompliance with cybersecurity standards required as a condition for payment under the contract (e.g., measures to protect governmental data or prohibitions on using components made in restricted foreign countries);
2. misrepresentation of security controls or practices to secure a government contract; and
3. failure to timely report suspected cybersecurity breaches or incidents.

Boynton stated that the DOJ had secured additional resources, including appointment of a supervisor within the DOJ's Civil Fraud Section to oversee the initiative. He promoted a new tool on the DOJ website with instructions on how to report cybersecurity complaints via hotline or seek legal counsel to file a whistleblower lawsuit. He also said that the DOJ had partnered with the offices of inspector general of numerous federal agencies to "promote information sharing and technical expertise, generate referrals for investigations, and multiply the number of experienced federal agents and attorneys dedicated to combatting knowing cybersecurity failures."

KEY TAKEAWAYS

- The DOJ has signaled that it is serious about using the FCA to act against federal contractors that have fallen short of cybersecurity requirements imposed as a condition for payment by the government.
- There are many sources of cybersecurity obligations for federal contractors, including statutes, agency regulations, and the contractor's written agreement(s) with the government. Companies that do business with the government—especially those who handle classified or other sensitive information and systems—should engage experienced counsel with expertise in cyber- and data-security issues to ensure they are aware of and complying with all applicable requirements.
- It is critical that federal contractors maintain robust compliance systems to swiftly detect and remediate—and, if necessary, timely report—any cybersecurity failures or breaches.

If you have any questions or need further assistance, please contact **Chase Cooper** (Associate, Complex Commercial Litigation) or your Winston & Strawn relationship attorney.

---

[1] *Universal Health Servs., Inc. v. United States ex rel. Escobar*, 136 S. Ct. 1989, 1995 (2016).

[2] *See, e.g.*, *United States ex rel. Markus v. Aerojet Rocketdyne Holdings, Inc.*, 381 F. Supp. 3d 1240, 1249 (E.D. Cal. 2019) (denying dismissal of an FCA claim where the relator adequately pleaded that defendant contractor's alleged failure to disclose its noncompliance with Department of Defense and NASA cybersecurity regulations "was material to the government's decision to enter into and pay on the relevant contracts").

4 Min Read

Author

Chase J. Cooper

Related Locations

Houston

Related Topics

Department of Justice (DOJ)

False Claims Act

Cyber Security

Related Capabilities

Privacy & Data Security

Government Investigations, Enforcement & Compliance

Government Program Fraud, False Claims Act & Qui Tam Litigation

Related Regions

North America

Related Professionals

Chase J. Cooper

This entry has been created for information and planning purposes. It is not intended to be, nor should it be substituted for, legal advice, which turns on specific facts.

© 2024 Winston & Strawn LLP.