CARLTON FIELDS

DOJ Unveils New Initiative to Pursue Cybersecurity-Related Fraud by Government Contractors and Grant Recipients

October 20, 2021

Introduction
Earlier this month, the Department of Justice (DOJ) announced the launch of its Civil Cyber-Fraud Initiative, aimed to combat cyber threats to the security of U.S. infrastructure. The initiative combines the DOJ's "expertise in civil fraud enforcement, government procurement, and cybersecurity" in a much-anticipated and well-predicted shift by the DOJ to rely on the federal False Claims Act (FCA) to enforce cybersecurity compliance.

The DOJ's decision to use the FCA as its enforcement tool is notable for several reasons. First, the broadly written FCA aims to reach all types of fraud resulting in financial loss to the government, including loss stemming from cybersecurity-related fraud. Second, the FCA creates monetary incentives that encourage qui tam actions (also known as "whistleblower" lawsuits). The DOJ's recent actions and statements send a clear signal to the federal contracting community: comply with cybersecurity requirements or risk liability under the FCA.

False Claims Act Overview

Every year, the government loses billions of dollars due to fraud. Congress enacted the FCA, 31 U.S.C. §§ 3729-3733, to reclaim these funds either through direct actions brought by the DOJ or by granting private individuals (known as "relators") the power to initiate legal action on the government's behalf.

FCA violations occur when the entity knows, or should know, it is committing material fraud. An entity knowingly commits fraud when it has actual knowledge of the information, acted in deliberate ignorance of whether the information was true or false, or acted in reckless disregard of the truth or falsity of the information. 31 U.S.C. § 3729(b)(1). In other words, an entity must have knowingly violated the FCA. In addition to the knowledge requirement, the FCA liability hook attaches only when the subject of the fraud is material to a government decision. Fraud is material when it "[has] a natural tendency to influence, or be capable of influencing, the payment or receipt of money or property." 31 U.S.C. § 3729(b)(4). Thus, an entity violates the FCA when it knowingly presents, or causes to be presented, a material false or fraudulent claim to the government. Such violations may occur when a contractor submits a bid to the government that includes certain assurances, such as its compliance with federal cybersecurity requirements, but the contractor is aware that it is likely noncompliant (or has chosen to ignore its cyber obligations).

The penalties for an FCA violation can be severe. The FCA allows up to three times the damages plus a significant civil penalty, ranging as high as $23,331, for each false claim. 31 U.S.C. § 3729(a)(1). Yet the government is not the only one that has a stake in the result. Relators may share up to 30% of the recovery, and if successful, reasonable attorneys' fees and costs. 31 U.S.C. § 3730(c).

False Claims Act in the Cybersecurity Context

In the cybersecurity context, a risk of FCA liability emerges when handling sensitive government information and making cybersecurity-related promises to government officials. A federal contractor or grant recipient incurs liability under the FCA when it puts U.S. information or systems at risk by *knowingly* (i) providing deficient cybersecurity products or services; (ii) misrepresenting its cybersecurity practices or protocols; or (iii) violating obligations to monitor and report cybersecurity incidents and breaches. For example, in *United States ex rel. Markus v. Aerojet Rocketdyne Holdings Inc.*, the relator alleged that the defendant falsely asserted its compliance with cybersecurity standards when entering into Department of Defense (DOD) contracts. The court refused to dismiss the FCA claims, holding that the relator had sufficiently pleaded 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." Thus, an entity conducting business with the government should be aware that a violation, or misrepresentation, of cybersecurity requirements heightens the risk of *qui tam* lawsuits and fraud investigations by law enforcement. Enhanced FCA activity in the cybersecurity arena is likely, in part, because relators receive protection from retaliation and monetary reward incentives.

FCA Liability Can Attach Without Proof of a Data Breach

A successful FCA enforcement action does not require proof of an actual data breach. Rather, liability may attach to the mere possibility of a breach. In the *United States ex rel. Glenn v. Cisco Systems Inc.* settlement, Cisco sold equipment to government agencies knowing that the equipment was vulnerable to a cyberattack. Although no breach occurred, Cisco still paid $8.6 million to resolve FCA claims stemming from alleged misrepresentations regarding cybersecurity risks.

To mitigate FCA liability risks, government contractors and grant recipients should consider conducting a cybersecurity risk assessment of their products and systems *before* contracting with the government. These risk assessments should continue regularly throughout the relationship with the government.

Because government cybersecurity requirements are extensive and evolving, meeting the requirements - and mitigating the associated FCA risks - can vary from contractor to contractor. For example, some contracts may require cybersecurity levels to mirror a government or industry standard, some require strict government controls, and many require compliance down the supply chain according to specific factors. Contractors should ensure they understand the various requirements at issue in their contract (e.g., required certifications or risk assessments) and consider the applicable risks before undertaking new requirements.

Steps to Mitigate Cyber-Related FCA Liability

All businesses should be cognizant that cybersecurity compliance will be subject to a heightened level of scrutiny by regulators and relators. To mitigate the risk of FCA liability, government contractors and grant recipients should:

- Record compliance efforts by maintaining cybersecurity training records and written policies and procedures, including an incident response plan.
- Continuously monitor compliance with applicable cybersecurity requirements and promptly remedy any existing security gaps or security incidents.
- Ensure all representations made to the government regarding cybersecurity capabilities and compliance adhere to the applicable requirements.

- Solicit internal cybersecurity feedback and educate employees on their obligations to comply with federal cybersecurity standards.
- Avoid retaliation against any employee or individual raising cybersecurity concerns.

Authored By

Adam P. Schwartz

Erin J. Hoyle

Eden Marcu

Related Practices

Cybersecurity and Privacy
Government Law & Consulting