CARLTON FIELDS

Recent Cases Indicate Viability of False Claims Act Liability Connected to Federal Cybersecurity Standards

January 09, 2020

Introduction

Government contractors are no strangers to the numerous quality standards and assurances required by the government. Over the past several years, cybersecurity in federal contracting has emerged as yet another standard to achieve. While data breaches are big news in the private sector, the issue remained somewhat under the radar for public contracts — until now.

Last summer, two significant whistleblower cases sent ripples through the False Claims Act (FCA) community by demonstrating the specter of FCA liability resulting from the failure to comply with cybersecurity requirements in government contracts. In May, the U.S. District Court for the Eastern District of California refused to dismiss a case alleging that Aerojet Rocketdyne Holdings Inc. falsely asserted its compliance with the Department of Defense's (DOD) cybersecurity standards. Then, in late July, the government announced that Cisco Systems Inc. agreed to pay $8.6 million to settle a whistleblower suit alleging that the company fell short of federal cybersecurity standards by selling video surveillance products with known vulnerabilities that hackers could exploit. These cases show that cybersecurity-based FCA claims may be the new frontier and that such claims may prove difficult to defeat depending on the facts in any given case.

False Claims Act Overview

The FCA, 31 U.S.C. §§ 3729–3733, prohibits the submission of false or fraudulent claims to the government. The statute imposes civil liability for knowingly (i) submitting a false or fraudulent claim for payment; (ii) causing such a claim to be submitted for payment; (iii) making, using, or causing to make or use a false record or statement material to a false or fraudulent claim; (iv) conspiring to get

such a claim paid or approved; or (v) making a false record or statement to conceal or avoid an obligation to pay money to the government. The act also imposes rigorous materiality requirements, defined as "having 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).

The FCA allows an individual, known as a relator, to bring a civil action on behalf of the government under the act's whistleblower, or qui tam, provisions. A relator files the complaint under seal in a federal district court and serves the government with a copy of the complaint and a written statement of all material evidence supporting the allegations. The complaint may remain sealed for 60 days while the government investigates the allegations. This seal is frequently extended for months or years before the case proceeds.

Before unsealing the complaint, the government notifies the relator and the court of whether it will become formally involved, or "intervene," in the case. If the government intervenes, the relator generally receives 15% to 25% of the government's recovery in the event of settlement or judgment in favor of the United States. If the government declines to intervene, the relator may independently proceed with the action and may receive 25% to 30% of any recovery. In addition, the relator is entitled to a separate award for reasonable attorneys' fees and costs.

Cases brought under the FCA can result in judgment of up to three times the amount of damages plus a monetary civil penalty per false claim. 31 U.S.C. § 3729(a)(1). The act requires a knowledge component, shown by (i) having actual knowledge; (ii) acting "in deliberate ignorance of whether the information is true or false"; or (iii) acting "in reckless disregard of the truth or falsity of the information." 31 U.S.C. § 3729(b)(1).

U.S. ex rel. Markus v. Aerojet Rocketdyne Holdings Inc.

The relator in *Markus* served as the defendants' senior director of cybersecurity from June 2014 to September 2015. The relator alleged that the defendants' computer systems failed to meet the minimum cybersecurity requirements necessary to receive a contract award funded by the DOD. The relator claimed that the defendants knew they were not compliant with the relevant standards as early as 2014, but that they repeatedly misrepresented their compliance with such technical standards to government officials. Based on those allegedly false and misleading statements, the government awarded one of the defendants a DOD-funded contract. The relator further alleged that the defendant employer wanted him to certify that the company was compliant with the DOD regulations when, in fact, it was not. The relator refused to sign the certification, contacted the company's ethics hotline, and filed an internal report.

The defendants apparently terminated the relator in September 2015, and the relator filed his initial complaint alleging violations of the FCA in October 2015. The United States declined to intervene in

the case. The defendants moved to dismiss the complaint, but the court denied the motion, holding that the relator "plausibly pled that defendants' alleged failure to fully disclose its noncompliance [with federal cybersecurity requirements] was material to the government's decision to enter into and pay on the relevant contracts."

The case stands for the proposition that cybersecurity compliance is, and will likely continue to be, a material aspect of contracts that require certification of compliance with (i) an articulated cybersecurity standard or (ii) "adequate" protections for data.

Cisco's $8.6 Million FCA Settlement

The Cisco settlement is believed to be the first FCA payout for a cybersecurity-related allegation. The relator initially filed the case under seal in 2011. According to the complaint, the relator tested a line of Cisco products in 2008 and discovered that there were security risks in the products' design. Cisco terminated the relator a few months after he submitted a report on the vulnerabilities of the product line and regularly followed up after receiving no response to his report. Despite this report, Cisco marketed and sold the surveillance products to federal government agencies.

In mid-2013, almost two years after the suit's filing, Cisco acknowledged that there were security vulnerabilities that may allow an attacker to gain full administrative privileges on the system, including the ability to alter camera feeds. There is no indication that those vulnerabilities were actually exploited. On July 31, 2019, the United States intervened in the suit for the purpose of settlement, joined by 15 states and the District of Columbia. Cisco subsequently agreed to settle the lawsuit without admitting any liability.

This settlement suggests that successful enforcement of a cybersecurity claim under the FCA may not depend on proof of an actual cyber breach; instead, the mere possibility of a breach could be sufficient. Additionally, companies must maintain a zero-tolerance policy for retaliation against cybersecurity whistleblowers. Retaliating against employees who report concerns internally may not only run afoul of FCA anti-retaliation provisions, but also could encourage those employees to file qui tam actions.

Conclusion

Companies contracting with the government must remain aware of the government's growing focus on cybersecurity compliance. Given the fast-paced developments in technology and increasing pressure to devise ways to counteract cyberattacks, contractors should demonstrate and document on an ongoing basis that they are assessing cybersecurity compliance and regularly updating their system security plans. By doing so, companies can more fully explain their compliance with cyber requirements, and potentially thwart allegations of a "knowing" violation of any compliance

standards. An effective compliance program can drive a robust cyber risk management process and promote an environment with zero-tolerance for retaliation.

Authored By

Adam P. Schwartz

Erin J. Hoyle

Related Practices

Cybersecurity and Privacy
White Collar Crime & Government Investigations