Cybersecurity Law Report

What to Know (and Do) About DOJ's Efforts to Identify and Prosecute Cybersecurity Fraud Under the False Claims Act

By Veronica Nannis, *Joseph Greenwald and Laake*

The DOJ has its sights set on cybersecurity fraud and is pursuing alleged offenders in unprecedented ways. Since establishing its Civil Cyber-Fraud Initiative in 2021, the DOJ has pursued several entities for cybersecurity fraud. In August 2024, it joined and took over a fraud case brought by a whistleblower – the first time the United States has taken the lead role in prosecuting a cybersecurity fraud case. This article summarizes the DOJ's efforts since 2021 and discusses what all cybersecurity contractors should do both to maintain compliance and avoid costly cyber-fraud investigations.

See "Revised DOJ Guidance Clarifies Liability Protections for Good-Faith Security Research" (Jun. 8, 2022).

The False Claims Act

To understand the recent cyber-fraud investigations, a basic False Claims Act (FCA) primer is in order. The FCA was established during the Civil War to combat defense contractor fraud on the United States, mostly in relation to wartime materials and resources. This "Lincoln's Law," passed in 1863, was first used to prosecute fraudsters profiting off the war effort by, among other actions, selling the Union Army crates filled with sawdust instead of muskets, sick mules, substandard uniforms and rotten food supplies. The FCA then sat relatively dormant after the Civil War until significant amendments in 1986, 2009 and 2010 greatly expanded and strengthened this unique law.

Whistleblowers and Their Incentive

Critically, and quite exceptionally, the FCA deputizes *private citizens* to file suit on behalf, and in the shoes, of the United States, to bring cases against individuals or companies allegedly defrauding it. These "private attorneys general" are called "whistleblowers" colloquially and "relators" under the FCA's *qui tam* provision. The term "*qui tam*" is abbreviated from the Latin phrase meaning, "He who sues in this matter for the King as well as for himself." Successful relators have first-hand knowledge and details of any alleged fraud on the government. Relators are typically former or current employees, vendors or even competitors of the defendants in FCA cases. So, while private citizen relators file suit initially and can prosecute these cases on their own, all relators try to get the government to take over the case and prosecute the fraud in its own right. When this is done, it is called government intervention.

Relators play a critical role in safeguarding the public good and taxpayer dollars by uncovering fraud schemes by those seeking to take advantage of government funds. They are duly incentivized to stick their necks out to blow the whistle on fraud. If there is a recovery by the United States, the relator who brought the case is entitled to between 15 and 30 percent of the collected proceeds. Given that these cases are frequently million-dollar recoveries, a relator's individual share can be substantial.

Four Elements of a Violation

An FCA violation contains four basic elements: (1) a false statement or fraudulent course of conduct; (2) made or carried out with knowledge of the falsity; (3) that was material (*i.e.*, material in the government's decision to pay a grant, program or claim, or to pay on a federal contract); and (4) that involved a claim (*i.e.*, demand for money or property from the United States). Generally, FCA liability exists for any person who knowingly submits a false claim, causes another to submit a false claim, knowingly makes a false record or statement to get a false claim paid by the government, or conspires to do the same. At its heart, the FCA is intended to recover ill-gotten gains and to deter fraudulent conduct.

Penalties

The modern FCA imposes strong penalties on fraudsters. For civil violations, a statutory penalty of no less than $13,946 and no more than $21,916 *per false claim* is possible as of February 2024. Damages are allowed to be trebled (tripled) under the FCA so that the United States can recoup three times what the government actually paid for each false claim. Fraudsters also can be suspended or debarred from any future participation in government programs. For instance, a health-

care company can be disbarred from Medicare, or a defense contractor can be prohibited from any further government contracts. Lastly, both companies and individuals can be prosecuted criminally (in addition to civil prosecution) for FCA violations, resulting in more fines and potential criminal charges in the more extreme cases.

Though government reporting shows that fraud continues to flourish, and still outpaces efforts to curb it, by any measure, the FCA has nevertheless been wildly successful. The Justice Department reported that settlements and judgments under the FCA exceeded $2.68 billion for fiscal year 2023. During that one year, the government and relators were party to 543 settlements and judgments – a record number in a single year. Since the 1986 amendments, the United States has recovered more than $75 billion under the FCA.

See "Ten Cybersecurity Resolutions for Financial Services Firms in 2023" (Jan. 11, 2023).

DOJ's Civil Cyber-Fraud Initiative and Related Proceedings

The FCA has been used to combat an eclectic mix of fraud, with cybersecurity fraud being one of the DOJ's more recent targets.

The Cyber-Fraud Initiative

The DOJ's effort to combat cybersecurity threats includes its Civil Cyber-Fraud Initiative (Initiative), which was announced in October 2021. The Initiative is dedicated to using the FCA to promote cybersecurity compliance by government contractors and grantees by holding them accountable when they "knowingly" violate applicable cybersecurity requirements. Acting "knowingly" under the FCA has a somewhat expansive definition. It includes: (1) actual knowledge of the information; (2) deliberate ignorance of the truth or falsity of the information; or even (3) reckless disregard of the truth or falsity of the information. Critically, a relator (or the government, if it intervenes) is *not* required to prove specific intent to defraud.

The Initiative has resulted in several investigations, settlements and litigations since its formation just three years ago.

Cyber-Fraud Settlements

Comprehensive Health Services

On March 8, 2022, the DOJ announced a $930,000 settlement with Comprehensive Health Services, LLC for alleged FCA violations. This settlement was the DOJ's first such resolution after launching its Initiative, and a harbinger of things to come. Observant cybersecurity contractors likely took heed.

Aerojet Rocketdyne

Then, in July 2022, the DOJ made more news with the announcement that Aerojet Rocketdyne Inc. agreed to pay $9 million to resolve allegations that it violated the FCA by misrepresenting its compliance with cybersecurity requirements in certain federal government contracts. Aerojet provides propulsion and power systems for launch vehicles, missiles, satellites and other space vehicles to the Department of Defense, NASA and other federal agencies. This case was brought under the FCA's *qui tam* provision by a former Aerojet employee, who received a $2.61-million share in the government's recovery. The DOJ highlighted this case as a prime example of "how whistleblowers can contribute to civil enforcement of cybersecurity requirements through the False Claims Act."

In its press release, Principal Deputy Assistant Attorney General Brian M. Boynton, head of the Justice Department's Civil Division, emphasized that, "whistleblowers with inside information and technical expertise can provide crucial assistance in identifying knowing cybersecurity failures and misconduct." Highlighting a whistleblower and his or her contribution and monetary award is typical of the DOJ's press strategy in announcing FCA settlements. This, it hopes, serves to incentivize future whistleblowers to come forward with their insider information about fraud on the government.

Jelly Bean

March 2023 saw the announcement of a settlement with Jelly Bean Communications Design LLC and its manager. While a relatively small amount for a settlement under the FCA, totaling just $293,771, cybersecurity contractors should not sleep on this settlement. It demonstrates that the DOJ is willing to pursue cyber-fraud allegations even if they are relatively low-dollar violations. The DOJ alleged that the defendants failed to secure personal information on a federally funded Florida children's health insurance website, which Jelly Bean created, hosted and maintained. The settlement resolved allegations that Jelly Bean did not provide the secure hosting of the applicants' personal information as contractually required, but instead, knowingly failed to properly maintain, patch and update the software systems. When the site was cyberattacked, the breach exposed the information of

500,000 applicants. Of note, the DOJ also individually named Jelly Bean's manager, 50-percent owner and sole employee, as a target of its investigation and party to the settlement. FCA cases are often against companies but can be equally brought against individuals as well.

Verizon

In September 2023, the DOJ settled for over $4 million with Verizon Business Network Services LLC. The settlement resolved FCA allegations that Verizon failed to completely satisfy certain cybersecurity controls in connection with an IT service provided to federal agencies under various different General Services Administration contracts. Strikingly rare, reportedly, Verizon voluntarily disclosed its actions, initiated an independent investigation and compliance reviews of all concerning issues, and remediated its cybersecurity failures. The United States acknowledged Verizon's disclosure and remediation efforts and cited this cooperation as the basis for providing Verizon with a "credit" in relation to the ultimate settlement amount.

The Verizon settlement demonstrates the DOJ's commitment to working with companies that self-disclose potential fraud and are transparent and cooperative with investigations. The DOJ has said, and this settlement underscores the message, that companies that self-disclose fraud will be afforded potentially significant credit for their cooperation. The DOJ has several programs incentivizing voluntary disclosure of fraud, including its 9-47.120 policy on corporate enforcement and voluntary self-disclosure, available on its website, and the Criminal Division's correlating Pilot Program on Voluntary Self-Disclosures for Individuals.

Guidehouse and Nan McKay and Associates

In June 2024, the United States publicized another settlement involving allegations that cybersecurity contractors failed to meet contractual requirements. Unlike those discussed above, this $11.3-million settlement involved a New York State contract meant to ensure a secure environment for low-income New Yorkers to apply online for federal rental assistance during the COVID-19 pandemic. Guidehouse Inc. paid $7.6 million while Nan McKay and Associates paid $3.7 million to resolve allegations that they violated the FCA. These settlements were the result of a case brought about by a former Guidehouse employee-turned-whistleblower, who received a $1,949,250 *qui tam* share of the settlement amounts. It is important to keep in mind that some 33 states have their own False Claims Acts, typically similar to the federal version. The state laws are used, as is their federal counterpart, to

combat fraud on the state governments. Whistleblower incentives and protections in most state FCAs mirror the federal provisions.

DoD's Special Audit Report

In December 2023, the Department of Defense Office of Inspector General (DoD OIG) issued a "special" Audit Report providing insight into common cybersecurity weaknesses related to the protection of Controlled Unclassified Information (CUI). The Audit Report recounts that between 2018 and 2023, DoD OIG issued five audit reports focused on DoD contractors' "inconsistent implementation of Federal cybersecurity requirements for protecting CUI that are contained in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171." The Audit Report also states that the DoD OIG has supported five DOJ investigations conducted under the Initiative.

The Audit Report recounts that DoD currently has more than 183,000 active contracts covering all sectors of the economy, many of which require contractors to process, store and/or transmit CUI on their own networks and systems. Through DFARS 252.204-7012, DoD requires its contractors handling CUI to implement, or have a plan to implement, the 110 security controls found in NIST SP 800-171; these cover a spectrum of subjects, including access controls, audit and accountability, incident reporting, physical protection and risk/security assessments. At its core, DFARS 252.204-7012 requires contractors to provide "adequate security" for CUI and imposes certain incident reporting obligations.

When a federal agency issues regulations or other guidance, government contractors should take note and follow them. All government contractors may be expected to adhere to DFARS 252.204-7012 requirements to protect CUI and could be held to account for related fraud. Government contractors could face penalties not only for failing to comply with their specific contract requirements, but also for failing to ensure compliance with all regulations and rules cited in guidance like the Audit Report.

See "Understanding and Implementing DoD's Cybersecurity Requirements" (Aug. 17, 2022).

Active Litigation of Cyber-Fraud Cases

Cybersecurity companies that do not cooperate or settle FCA investigations often find themselves in active litigation with or without the United States' intervention. The two most closely watched 2024 cases are against higher education institutions.

Penn State

A case pending against Penn State University based on alleged cybersecurity failures was brought by a relator and, at the time of this writing, is stayed while the United States considers intervention. The whistleblower in this case is the former CIO for Penn State, who was hired after a breach to review and ensure cyber compliance. The relator alleges that Penn State knowingly failed to comply with numerous cybersecurity controls that are required for DoD contractors by DFARS 252.204-7012.

Interested observers should keep an eye on the Penn State case regardless of the United States' intervention decision. More and more whistleblowers and their counsel are deciding to litigate strong FCA cases without the United States' intervention. While most litigated FCA cases are settled out of court (given the significant risk to defendants from an adverse trial verdict), some are tried before juries. It is possible that one of the cyber-fraud FCA cases pending right now will eventually be the first to go to a jury trial wherein the defendant risks significant statutory damages, penalties and fees if it loses.

Georgia Tech

The other pending cyber-fraud litigation, against the Georgia Institute of Technology (Georgia Tech), is based on allegations that the school misrepresented compliance with several cybersecurity regulations governing what contractors must do to protect government information on its systems. Ironically, the complaint alleges lax cybersecurity standards at the Georgia Tech research lab that focuses on cybersecurity and cyberattack attribution for multiple U.S. defense contracts. This case was brought by a pair of relators who were previously senior members of Georgia Tech's cybersecurity compliance team. It is the first FCA case in which the United States has intervened against a higher education institution for failing to comply with contractual cybersecurity requirements.

The United States filed a scathing Complaint in Intervention in August 2024 that cites Georgia Tech's employees' testimony during the investigation and quotes generously from internal communications, including instant messages. The United States alleges that for many years there was "no enforcement" of cybersecurity regulations at Georgia Tech and that the defendant knew that the lack of this compliance resulted in "false claims" being submitted to the United States. The government claims that one of the reasons Georgia Tech failed to comply with cybersecurity regulations and requirements was because they were "too burdensome."

Among its fraud claims, the United States alleges that Georgia Tech failed to: (1) develop or implement a system security plan outlining how it would protect against unauthorized disclosure of sensitive, covered defense information in its possession; (2) install, update and run anti-virus software on its various devices; (3) assess its system on which sensitive DoD data was processed, stored or transmitted; and (4) provide DoD with an accurate summary level score to demonstrate its lab's compliance with applicable cybersecurity regulations. The failure to provide a score was because, the United States alleges, no such score ever existed for its lab, and the one reported to DoD was "fictitious" or "virtual." Armed with two former cyber compliance employees as relators and with what appears to be significant and detailed evidence to support its allegations, the United States seems, at this stage of the proceedings, to be on solid footing in pursuing this case. All cyber professionals should follow this case, watch for developments and study its allegations while comparing their own policies and actions against those contained in cases like this one.

Mitigating Risk

The federal and many state governments incentivize relators to bring forth detailed allegations of fraud, as several of the examples discussed in this article demonstrate. The United States wants to hear from relators with personal knowledge of fraud and has shown a great willingness to work with relators or even intervene on these cases. Simultaneously, governments actively encourage recipients of government funds to be vigilant in combatting fraud by ensuring compliance with all applicable laws, rules, regulations and contract terms. Just as relators are awarded a portion of recoveries in successful FCA cases, target companies are also afforded credit for having meaningful compliance policies and for self-disclosing fraud.

What can cybersecurity contractors proactively do to avoid fates similar to those highlighted herein?

Stay Educated

In addition to reviewing the cases and reports discussed in this article, smart contractors should keep apprised of new cyber-fraud cases and carefully follow the pending cases as they make their way through the courts. There should be lessons learned from every cyber-fraud settlement and litigation announced. Each one is a new opportunity for contractors to review and update their compliance policies and controls.

See this two-part series on getting started with CMMC: "Understanding Goals, Requirements and Challenges" (Jan. 27, 2021), and "How to Prepare and What to Expect From the Assessment" (Feb. 3, 2021).

Review, Update and Train All Staff on Compliance Policies

Real, transparent and robust compliance programs are critical. Special attention should be paid to all applicable federal laws, regulations, and guidance in creating and routinely updating these policies. Once current, meaningful compliance policies are established and documented, then mandatory yearly training on the policies must follow.

See "Tesco Is Making Big Strides With Little Learning Leaps" (Jun. 1, 2022).

Listen to, Investigate and Take Action Following Internal Complaints

Careful notice, investigation and timely follow-up are crucial following any internal reports of suspected fraud. In most cases, whistleblowers try to address and correct suspected fraud internally before they ever reach the step of reporting to the government. By conducting meaningful and thorough investigations into fraud allegations and voluntarily disclosing potential wrongdoing, contractors may be able to avoid costly and high-profile investigations and FCA litigation.

See "Navigating the Intersection of Whistleblowing and China's Data Protection Regime" (Apr. 12, 2023).

Veronica Nannis is a shareholder at Joseph Greenwald and Laake PA, with nationwide experience representing whistleblowers and litigating False Claims Act cases. In 2023, she represented a whistleblower claiming Medicare fraud against an Indiana hospital, which settled the matter by paying the government $345 million, a record-setting settlement for a case based on the Stark Law.