# Cyber Whistleblowers—Eight Lessons from the First False Claims Act Settlements

**July 21, 2022**

On July 8, 2022, the U.S. Department of Justice (the "DOJ") announced that Aerojet Rocketdyne ("Aerojet"), a California-based aerospace and defense contractor, agreed to pay $9 million to resolve allegations that it violated the False Claims Act (the "FCA") by misrepresenting its compliance with cybersecurity requirements in federal government contracts. The DOJ's announcement follows the court's approval of a tentative settlement reached on April 27, 2022 by Aerojet and the whistleblower who filed the claims. This is the second settlement of cybersecurity-related FCA claims since the DOJ's announcement of its new Civil Cyber-Fraud Initiative in October 2021, although the claims were brought against Aerojet well before the initiative was launched.

## The *Aerojet* Settlement

The July 2022 *Aerojet* settlement resolved claims first filed in 2015 by a senior cybersecurity official at Aerojet who alleged that the company entered into contracts with the Department of Defense ("DoD") and NASA despite knowing that it did not meet the regulatory cybersecurity requirements. The whistleblower claimed to have filed the action after his attempts to raise the issue through internal channels proved unsuccessful.

Specifically, the whistleblower alleged that Aerojet failed to comply with (and materially misrepresented the extent to which it complied with) DoD and NASA regulations requiring it to safeguard certain unclassified information from cybersecurity threats. Aerojet argued that it had disclosed its noncompliance before entering into the contract and that any noncompliance with relevant cybersecurity requirements was immaterial to the contract.

In 2019, a California federal court denied Aerojet's motion to dismiss the claims and, in 2022, denied Aerojet's motion for summary judgment, finding that partial disclosures would not relieve Aerojet of liability if it nonetheless failed to disclose its noncompliance with material regulatory provisions. Following the second day of a jury trial, Aerojet and the whistleblower reached a $9 million settlement to resolve all claims.

## The DOJ Civil Cyber-Fraud Initiative

The *Aerojet* settlement comes as the Biden administration has increasingly emphasized the need to combat emerging cyber threats. On October 6, 2021, Deputy Attorney General Lisa Monaco announced the launch of the DOJ's Civil Cyber-Fraud Initiative, which seeks to deter cyber vulnerabilities and prevent attacks through FCA cases against government contractors who fail to meet required cybersecurity standards. While the DOJ opted not to intervene in *Aerojet* in 2019, it filed a statement of interest in response to Aerojet's motion for summary judgment, arguing that Aerojet's ability to safely maintain government data was critical to the contract.

The DOJ has identified three primary targets for its FCA enforcement efforts: (1) failure to comply with cybersecurity requirements; (2) misrepresentations of cybersecurity controls and practices; and (3) failure to report suspected data breaches in a timely manner as required by contract. These priorities underscore that it is critical for companies to ensure they have complied with all applicable cybersecurity requirements each time they submit bids for federal contracts or claims for federal funds.

At first glance, the Civil Cyber-Fraud Initiative appears to apply primarily to defense contractors such as the defense industrial base, but regulations covering cybersecurity requirements apply to a much broader group than just those identifying themselves as "defense contractors." For example, on March 8, 2022, Comprehensive Health Services, LLC ("CHS") agreed to pay $930,000 to resolve claims brought by the DOJ through the Cyber Civil-Fraud Initiative. The government alleged that CHS entered into an agreement with the government that included secure storage of confidential health records but failed to securely store the data or disclose the failures. Indeed, any company entering into a contract with the government that is subject to cybersecurity requirements may find itself making representations about its cybersecurity posture that could give rise to FCA claims.

These two settlements represent a new front in the cybersecurity regulatory compliance and enforcement battles. In the past two decades, the DOJ has taken steps to foster more collaboration with companies in cybersecurity defensive measures and threat intelligence sharing. Now, it appears that the DOJ's civil section may, at times, be at odds with companies over cybersecurity issues.

## Key Takeaways

In order to mitigate the risk of liability under the FCA and better prepare for and respond to cybersecurity-related whistleblower complaints in general, companies should consider the following:

- **Material Omissions Can Trigger Liability:** As demonstrated by the claims at issue in *Aerojet*, material omissions may be sufficient to assert liability under the FCA. In 2016, the Supreme Court recognized in *Universal Health Services, Inc. v. United States ex rel. Escobar*, the validity of "false implied certification" liability, holding that contractors may be liable for implicitly certifying compliance with federal regulations if they (1) submit a claim that makes specific representations about the goods or services provided, and (2) fail to disclose noncompliance with material statutory, regulatory, or contractual requirements rendering those representations misleading half-truths. While Aerojet had apparently disclosed to the government that it was not compliant with applicable cybersecurity standards, it allegedly failed to disclose the extent of that noncompliance. In particular, the whistleblower asserted that Aerojet failed to report its status on all required controls, made misstatements as to its partial compliance, and cherry-picked some of the data it shared with the government.

- **Cybersecurity Need Not Be Central to the Contract:** The *Aerojet* claims also demonstrate that misrepresentations about compliance with cyber requirements can form the basis of an FCA claim, even if cybersecurity is not the primary focus of the contract. The court rejected Aerojet's argument that the challenged omissions were not material because the contract related to missile defense and rocket engine technology—not cybersecurity. The court reasoned that Aerojet's alleged failure to comply with applicable cybersecurity regulations could have influenced its ability to handle technical information and therefore the extent to which it was able to fulfill the contract.

- **Penalties May Be Steep:** The FCA mandates both treble damages and penalties, which are periodically adjusted for inflation. As of May 2022, penalties under the FCA start at $12,572 and can reach $25,076 *per false claim*. Moreover, numerous circuits do not require a finding of damage to the government in order to maintain an FCA claim. As a result, those liable under the FCA can accumulate considerable financial penalties even before damages are considered. In 2021 alone, the DOJ recovered over $5.6 billion in settlements and judgments in FCA cases, $1.6 of which came from *qui tam* suits. Similarly, in 2020, the DOJ recovered over $2.2 billion in FCA actions, $1.7 billion of which was through *qui tam* suits in particular.

- **Whistleblowers Will Likely Have a Larger Role:** A key component of the FCA is its *qui tam* provision, which provides private citizens with a qualified right to bring FCA claims on behalf of the government, and allows them to recover up to 30% of the total judgment or settlement. After a whistleblower files a claim under the statute, the government may opt to join the action or allow the whistleblower to proceed alone. Consequently, current or former employees of a government contractor are able to leverage these protections to "blow the whistle" on their company's allegedly deficient cybersecurity policies, procedures, and practices, regardless of whether an incident has occurred.

  DOJ is not the only regulator leveraging whistleblowers. In October 2021, New York State amended its Labor Law to increase its whistleblower protections. As of July 15, 2022, the Securities and Exchange Commission has awarded approximately $1.3 billion to 276 individual whistleblowers, suggesting that, as the Commission expands its regulatory authority over cybersecurity, data management and AI, whistleblowers may be a key source of cases.

- **Consider Whistleblowers in Incident Response and Planning:** The technical, industry and company-specific expertise that whistleblowers can provide often makes them particularly useful to complex cybersecurity investigations. While whistleblower complaints may be vague or inflammatory, it is critical that companies take them seriously. As we have previously written, companies should maintain internal whistleblower channels, investigate all employee complaints regarding potential cybersecurity deficiencies with diligence, and refrain from taking any retaliatory actions against whistleblowers.

- **Maintain a Robust Cybersecurity Program:** Although the specific cybersecurity standards written into federal contracts or incorporated through regulations may vary and evolve, the *Aerojet* settlement, and the launch of the Cyber-Fraud Initiative, highlights the importance of establishing and maintaining a robust cybersecurity program. Many standard cybersecurity best practices (such as implementation of multifactor authentication, the Principle of Least Privilege, and segregation of duties) are mandated by commonly applicable federal frameworks and regulations. As such, a robust cybersecurity program allows federal contractors to more effectively manage cybersecurity risk generally and risk of liability under the FCA in particular.

- **Scrutinize Your Compliance:** Many companies have struggled to identify the proper role for their Compliance functions in cybersecurity. Some Compliance departments have taken a hands-off approach to cybersecurity, citing the subject-matter expertise of the information security office as critical and relying on that expertise to certify compliance. But with the increasing regulatory frameworks around cybersecurity,

bringing compliance into the fold and leveraging their expertise in compliance testing is critical as a way forward.

- **Scrutinize Subcontractor Compliance:** Both federal contractors and subcontractors can face liability under the FCA. As a result, companies should consider scrutinizing both their own and their subcontractors' compliance with any relevant cybersecurity requirements in order to manage the risk of FCA liability. Similarly, subcontractors should also take steps to identify cybersecurity requirements to which they are subject by virtue of their relationships with prime contractors. The risk subcontractors face under the FCA is exemplified by the $11.4 million 2015 settlement with NetCracker Technology, a DoD subcontractor, to resolve claims that it had knowingly used employees without required security clearances to perform work pursuant to a federal contract.

* * *

To subscribe to our Data Blog, please click here.

*The authors would like to thank law clerk Eli Goldman for his assistance on this Data Blog post.*

Please do not hesitate to contact us with any questions.

NEW YORK

Avi Gesser
agesser@debevoise.com

Erez Liebermann
eliebermann@debevoise.com

SAN FRANCISCO

H Jacqueline Brehmer
hjbrehmer@debevoise.com