2 FCA Settlements Highlight Gov't Cyber Liability Focus

By **Danny Ashby, Amanda Santella and John Dermody** (May 31, 2022)

Danny Ashby

Amanda Santella

John Dermody

Amid a swirl of high-profile cyber incidents and government warnings about cyber threats to critical infrastructure, two recent False Claims Act settlements related to cybersecurity point to a new front of potential cyber liability for companies doing business with the government.

On March 8, the U.S. Department of Justice reached a $930,000 settlement with Comprehensive Health Services LLC for falsely attesting that it properly secured medical records relating to U.S. Department of State and U.S. Department of Defense contracts.

And on April 27, Aerojet Rocketdyne Holdings Inc. reached a **settlement** with FCA relator Brian Markus who alleged that Aerojet lied to the Department of Defense and NASA about the protections it had in place for sensitive information.

These two cases, which we discuss in further detail below, are likely the initial wave of FCA cases related to cybersecurity representations.

The FCA is the federal government's primary vehicle for enforcing against fraud in government contracts, and the scope of potential defendants is sweeping: Any entity that does business, directly or indirectly, with the government can be held liable for submitting or causing the submission of a false or fraudulent claim for payment, or a false certification of compliance with a material legal requirement.

Moreover, the FCA's qui tam provision allows private relators to sue on behalf of the government and share in any recovery, providing a significant financial incentive for private parties to allege FCA violations — indeed, the vast majority of FCA actions are initiated by qui tam relators, making the relators bar a force multiplier in FCA enforcement.

Those financial incentives are bolstered by the FCA's treble damages provision, which can lead to large financial damages in cases where there is a recovery. In the last 10 years, the government has recovered nearly $38 billion under the FCA, mostly in cases against healthcare and life sciences defendants, which accounted for about $32 billion of that total.

But the DOJ has recently signaled a new priority for FCA enforcement: Announced in October 2021, the DOJ's Civil Cyber-Fraud Initiative seeks to hold accountable companies that put U.S. information or systems at risk by "knowingly providing deficient cybersecurity products or services, knowingly misrepresenting their cybersecurity practices or protocols, or knowingly violating obligations to monitor and report cybersecurity incidents and breaches."

Although the DOJ has so far only announced one settlement under the initiative, there are likely other pending cases that are not yet public because FCA actions are initially filed under seal — and often remain under seal during lengthy DOJ investigations. In public comments, the DOJ has actively encouraged the relators bar to bring more cases that DOJ

can pursue.

At first blush, the Comprehensive Health Services case might not seem the perfect fit as the first case under the Civil Cyber-Fraud Initiative. It stems from actions that occurred between 2012 and 2019 and relates to negligent handling of medical records and the provision of unauthorized medical care to State Department and U.S. Air Force personnel in Iraq and Afghanistan. But there are aspects of the case that are indicative of how the U.S. government is likely to pursue future FCA enforcement matters.

The case was a collaborative effort between the DOJ, the State Department's Office of Investigations, and the Air Force Office of Special Investigations. The involvement of AFOSI, in particular, reflects the priority that the Department of Defense has placed on cybersecurity issues, and the willingness to commit resources to these types of civil recoveries. It is likely that defense contractors will continue to be an enforcement priority, and there are certainly other cases already in the pipeline.

In addition to committing DOJ and Department of Defense resources, the government is counting upon a motivated relators bar to amplify their cybersecurity efforts. Although the DOJ declined to intervene in the Aerojet case in 2018, that was before the Civil Cyber-Fraud Initiative, and there is no doubt that the DOJ was watching the Aerojet case closely.

The relator in the case was the former senior director for cybersecurity, compliance and controls, who alleged that he was fired after he refused to sign documents asserting that Aerojet was compliant with government cybersecurity requirements. After an extensive procedural history, which included the dismissal of some claims, the parties reached a settlement on the second day of trial, after the relator had begun testifying.

The success of the relator in the Aerojet case likely portends an increase in similar claims. Cyber and data security requirements have been a component of government contracts for years, and there has long been a suspicion among government cybersecurity professionals that contractors have not been living up to their obligations, notwithstanding their certifications.

Such concerns are, in part, why the Department of Defense is implementing the Cyber Maturity Model Certification program, which will replace some aspects of the self-attestation approach with a third-party certification requirement. The CMMC is still in its infancy and limited to the Department of Defense, but other departments and agencies are adopting more aggressive postures in policing their cybersecurity requirements.

This increased focus is part of a broader government effort to make the private sector more resilient to cyber threats. As SolarWinds Corp. and the Microsoft Exchange exploitations vividly demonstrated, the government cannot protect its information without its contracting partners also securing their systems.

In SolarWinds, Russian intelligence services inserted a backdoor into a widely used network management software, and while their target was likely government information, it infected thousands of private sector users. And the Chinese Ministry of State Security exploited a flaw in Microsoft Exchange servers to gain access to tens of thousands of computers and networks around the world.

From the DOJ to the national cyber director, to the U.S. Department of Homeland Security and Congress, improving the cybersecurity of critical infrastructure and government contractors is being treated as a national security imperative. Consequently,

the DOJ is investing resources to investigate and bring high-profile cyber FCA cases not just to punish instances of fraud, but as a means to pressure government contractors to improve cybersecurity generally across industry.

For a motivated government and incentivized relators bar, cybersecurity noncompliance is a target-rich environment. Companies need to understand the ramifications of the cybersecurity and data protection clauses they are agreeing to in government contracts, whether as a prime- or subcontractor.

These clauses, such as Federal Acquisition Regulation 52.204-21 and Defense Federal Acquisition Regulation Supplement 252.204-7012, impose physical and cybersecurity obligations on contractor systems that process government information.

Not only do companies need to understand their cybersecurity obligations and take appropriate steps to ensure that they are living up to those standards, they need to understand their data inventory and which data is controlled unclassified information or is otherwise subject to these contractual protections.

And again, the FCA potentially affects every party in the government contracting chain, including subcontractors: In the healthcare space, for instance, the DOJ has recovered FCA damages from electronic health record vendors that did not directly contract with the government but that misrepresented the capabilities of their software to other parties who then certified that their systems were compliant with government requirements.

Conducting a privileged internal review is one way to assess the scope of potential FCA exposure and develop an approach to mitigate risk before your company is the target of a qui tam complaint or DOJ enforcement action.

Companies also need to invest time and resources in internal personnel management. Cybersecurity can, at times, be more art than science, and it is possible there will be differences of opinion among business, compliance and IT teams regarding the sufficiency of cybersecurity measures.

Such disagreements, if not addressed, can metastasize into potential FCA claims, which can be expensive and time-consuming to resolve even if they are without merit. Developing clear expectations and a robust compliance program can help identify deficiencies before they result in liability.

And an appropriate internal monitoring program can help detect unauthorized exfiltration of sensitive information by a disgruntled employee seeking to exploit the company.

The cybersecurity environment is changing. In addition to having to comply with new incident reporting regulations, companies need to invest sufficient time and resources to ensure they are living up to their contractual cybersecurity obligations. It won't just be a security incident that exposes a failure to do so; it will also be the government and relators imposing massive financial penalties on a company as a result.

Danny Ashby is a partner, and Amanda Santella and John Dermody are counsel, at O'Melveny & Myers LLP.

of the firm, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.