LOS ANGELES & SAN FRANCISCO
Daily Journal
www.dailyjournal.com
MONDAY, NOVEMBER 1, 2021

PERSPECTIVE

DOJ turns to familiar tool to address cybersecurity threats

By James Zelenay Jr., Eric Vandevelde and Tim Biché

As part of the Biden administration's ongoing efforts to modernize and bolster the nation's cybersecurity practices, last month, the Department of Justice launched a new Cyber-Fraud Initiative. The initiative will be led by the Fraud Section of the Civil Division's Commercial Litigation Branch and will look to deploy the False Claims Act against government contractors that put data at risk through the use of deficient cybersecurity products and services, by misrepresenting their cybersecurity practices or protocols, or by failing to monitor and report cybersecurity incidents.

The DOJ's announcement marks an innovative application of the FCA, which since the Civil War has been the go-to tool for recovering government funds obtained by fraud. Under the FCA, government contractors are liable for knowingly submitting false or fraudulent claims for payment to a government agency. The FCA is broad and can apply to a wide range of fraudulent conduct. While the FCA imposes liability only when an entity "knowingly" submits a false claim, the statute defines "knowledge" expansively, and defendants can be liable if they are deliberately ignorant of, or recklessly disregard, the truth or falsity of their claim for payment. Contractors that violate the FCA face significant monetary repercussions, including treble damages, penalties of more than $23,000 for each claim for payment, and attorney fees and costs.

One of the most distinct aspects of the FCA is the incentives it provides to whistleblowers to pursue claims on the government's behalf. Lawsuits brought by private parties, known as qui tam actions, are initially field under seal, and the government has the opportunity to intervene to take over such cases. Even if the government declines to intervene, the whistleblower can continue the action on his or her own, and successful whistleblowers can recover up to 30% of any damages that are awarded to the government. Qui tam actions make up the lion's share of FCA enforcement, accounting for more than 80% of FCA actions brought in the last 10 years.

While the launch of the DOJ's Cyber-Fraud Initiative represents a major shift in how the government will look to enforce cybersecurity regulations, it will not be the FCA's first appearance in the cyber arena. In 2018, a former employee of a government contractor brought a qui tam action alleging that the contractor knowingly misrepresented its compliance with certain cybersecurity requirements. *United States ex rel. Markus v. Aerojet Rocketdyne Holdings, Inc.*, 381 F. Supp. 3d 1240 (E.D. Cal. 2019). Even though the contracts at issue did not directly pertain to cybersecurity, the district court determined that the contractor's alleged failure to comply with cybersecurity requirements could have impacted the contractor's ability to perform the work specified under the contract, and denied the defendant's motion to dismiss. Notably, this was a qui tam matter in which the United States declined to intervene. Moreover, in 2019, the United States, along with a number of individual states, settled claims under the FCA and similar state law provisions alleging that a contractor sold video surveillance systems that were susceptible to hacking. *United States, ex rel. Glenn v. Cisco Sys., Inc.*, 1:11-cv-00400-RJA (W.D.N.Y.).

The DOJ's recent announcement suggests that the United States will both be more willing to intervene in qui tam actions based on alleged failure to comply with cybersecurity regulations and look to investigate and bring more of these cases on its own. But the increased use of the FCA to enforce cybersecurity regula-

James Zelenay Jr. *is a partner at Gibson, Dunn & Crutcher LLP.*

Eric Vandevelde *is a partner at Gibson, Dunn & Crutcher LLP.*

Tim Biché *is an associate at Gibson, Dunn & Crutcher LLP.*

tions raises important questions that government contractors will need to consider.

First, the precise cybersecurity standards that apply to federal contractors are in a state of flux. There are already myriad cybersecurity standards that could apply to contractors, including those in the Federal Acquisition Regulation, the Defense FAR Supplement, regulations promulgated by contracting agencies, and statutory requirements such as those set forth in HIPAA. It is also possible that the DOJ, and ultimately the courts, may look to the cybersecurity framework set forth by the National Institute of Standards and Technology for guidance. And on top of these preexisting standards, there are multiple bills in Congress that would impose new cybersecurity reporting requirements for federal contractors. Additionally, President Joe Biden's May 2021 Executive Order on Improving the Nation's Cybersecurity tasked a number of federal agencies with proposing new regulations for protecting digital data and requiring disclosure when data is compromised. Given the evolving nature of the regulatory landscape, contractors must be aware of their obligations both in terms of maintaining adequate cybersecurity and in reporting possible cybersecurity breaches.

Second, given the evolving landscape of these requirements, there will be important questions as to the facts needed for a whistleblower or the government to establish a defendant's scienter under the FCA. The FCA does not punish garden-variety regulatory violations. Instead, the violation must be one that is the result of "fraud." But "fraud" under the FCA includes submitting a false claim or statement with reckless disregard for the veracity of the claim or statement. How DOJ and courts grapple with whether a defendant's statement was "knowingly" false under the FCA — in light of the evolving landscape of cybersecurity requirements — will be an important development to watch.

Third, if a contractor is found to have knowingly submitted a claim falsely certifying compliance with cybersecurity requirements, questions of whether the alleged violation was material and how the government's damages will be measured will be critical. Under the Supreme Court's decision in *United Health Services v. United States ex rel. Escobar*, 136 S. Ct. 1989 (2015), the materiality element under the FCA — which asks whether the alleged improper conduct was actually material to the government's decision to pay a claim — is "rigorous" and "demanding." Further, under the FCA, the government's actual damages typically are how much more the government paid as a result of the alleged false certification. But will whistleblowers or the DOJ be able to show that compliance with evolving cybersecurity requirements was actually material to the government's decision to pay for a good or service, particularly if the good or service is unconnected with cybersecurity? And what is the cost in terms of damages of data being slightly more vulnerable to attack than it otherwise should be?

It is clear that the federal government is looking to shore up cybersecurity and to incentivize contractors to do the same. The DOJ's new enforcement priorities, along with the shifting regulatory landscape, combine to create unsettled waters that federal contractors should carefully navigate and consult with counsel as needed.