Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

DOJ Cybersecurity Crackdown May Inspire Whistleblowers

By **Daniel Wilson**

Law360 (October 8, 2021, 8:50 PM EDT) -- The U.S. Department of Justice's recent decision to crack down on federal contractors' cybersecurity shortcomings by using the False Claims Act sends a signal to whistleblowers that they can expect the government's support for reporting their employers.

On Wednesday, Deputy U.S. Attorney General Lisa Monaco announced the new Civil Cyber-Fraud Initiative, which will rely on the FCA to pursue cybersecurity-related fraud claims against federal contractors for putting "U.S. information or systems at risk."

The enforcement program will likely lead to a slew of new cases from qui tam whistleblowers, who file the vast majority of FCA cases, including those who may have considered doing so in the past but were put off by the amount of work required.

"It's more likely now that the Justice Department will do [whistleblowers'] work of investigating and developing a case, as opposed to in the past, [where] they had to do all the work themselves," said Susan Warshaw Ebner, a partner at Stinson LLP who also co-chairs the National Defense Industrial Association's Cyber Legal Policy Committee.

"So now it's an easy [decision] — let me raise the allegation, and then Justice will do the work to prove whether or not I was right," Ebner added.

The deputy attorney general also emphasized that the FCA protects whistleblowers from retaliation, which indicates to potential relators, "We're not just going to let the chips fall where they may with these kinds of things; we will actively help you," said Covington & Burling LLP senior of counsel Bob Huffman.

Monaco did not give any specific impetus for the initiative, other than to say that companies have for too long "chosen silence under the mistaken belief that it is less risky to hide a breach than to bring it forward."

But it follows in the wake of high-profile cybersecurity incidents such as the SolarWinds hack, a December 2020 cyberattack on the software company by that name that led to cybersecurity breaches at hundreds of client companies and at least nine federal agencies, and a May attack on the Colonial Pipeline Co., which temporarily shut down one of the U.S.' largest fuel pipelines.

It also comes as federal agencies, led particularly by the U.S. Department of Defense, have stepped

up cybersecurity requirements for contractors in recent years. During that time, the DOJ has attempted to avoid being adversarial toward contractors that are victims of cyberattacks, giving them opportunities instead to work to improve their cybersecurity, but its patience appears to have run out, McCarter & English LLP government contracts practice co-chair Alex Major said.

"I think for the past nine years that they've given contractors a lot of space to work with them," Major said. "I really do feel that they're maybe kind of exasperated and as a result are being very clear and very forward that 'we are doing this now, we're looking at this, we're taking it seriously.'"

The types of allegations the DOJ may pursue and the circumstances that may lead to enforcement actions are not entirely clear, beyond a few broad categories of behavior that Monaco set out in her speech. Those include the provision of deficient cybersecurity products or services, misrepresentation of cybersecurity practices, and violations of obligations to monitor and report cybersecurity incidents and breaches.

Ebner pointed out that "there is no such thing as complete cybersecurity," and it is unclear whether the DOJ will always treat contractors hit with a cyberattack or breach, despite their best efforts, as having inadequate security.

Another open question is whether there will be any sort of leniency for contractors that are victims of a breach if they fall afoul of timely notice requirements by first focusing on resolving and mitigating the breach, said Tina Reynolds, co-chair of Morrison & Foerster LLP's government contracts and public procurement practice.

"I think it would be a shame to punish them for not doing that strictly in accordance with their contractual requirements in the face of a crisis situation like that," she said.

Monaco also said that contractors could face "very hefty fines" for failing to adequately protect sensitive government systems, and there are a number of ways that could be interpreted.

That could refer to the FCA's civil penalty provisions, and may mean that the DOJ is willing to pursue cybersecurity-related cases with minimal actual damages if the civil penalties are significant enough, especially if it is trying to set an example of the types of behavior it is trying to curb.

Those civil penalties range from roughly $11,000 to $23,000 per false claim, and can quickly add up if the DOJ takes a particularly expansive view of potential liability, said Covington partner Susan Cassidy, co-chair of the firm's aerospace and defense industry group.

"DOJ has in the past had all kinds of theories of liability, where every invoice you submit after a breach is a violation, potentially … and there's no reason, I think, that they wouldn't consider that [approach] moving forward," she said.

But the DOJ's resources aren't limitless, and the department is still most likely to pursue the cases that its attorneys view as addressing the most egregious behavior, or providing the most "bang for the buck," according to Reynolds.

"I don't know that we'll see widespread cases that are not as strong as they would pursue otherwise," she said.

Also, FCA penalties are not generally considered to be fines, so Monaco could be referring to proposed mechanisms in pending legislation that would require companies to report any cyber breaches to the government quickly, or face fines, Reynolds said.

Amid the DOJ's "siren call to plaintiffs' counsel," contractors will need to be vigilant to ensure that their employees fully understand their obligations in regard to controlled unclassified information and covered defense information, or CUI and CDI, the types of information that contractual cybersecurity requirements are usually aimed at protecting, according to Major.

Listening to internal information technology and information security staff will also be key for minimizing potential FCA liability, because "they are the ones that are going to be either impugned or empowered to address this," Major said.

"And if they feel belittled, if they feel put upon, if they feel like they don't have a seat at the table, then I believe that is where a predominant amount of relators will stem from," he said.

There are only a few whistleblower FCA cybersecurity cases that have been brought so far — or at least only a few that aren't still under seal. But at least one of those cases, involving defense contractor Aerojet Rocketdyne, has shown that employee dissatisfaction can come from high up within the company, Hogan Lovells senior associate Stacy Hadeka said, while noting that the DOJ's initiative may prompt company leaders to take internal cybersecurity feedback more seriously.

The Aerojet case, allowed to move forward in a noteworthy 2019 ruling and still ongoing, was filed by the company's former senior director of cybersecurity, compliance and controls, who alleged Aerojet misrepresented its compliance with the DOD's cybersecurity standards.

"I've personally had experience where several clients have struggled to get buy-in from the top level, so now they have a lightning rod that they can take to their leadership, to use this as a way to push forward compliance and investment in cybersecurity compliance," Hadeka said.

--Additional reporting by Elise Hansen and Ben Kochman. Editing by Robert Rudinger.
