AMERICAN HEALTH LAW ASSOCIATION

HEALTH LAW WEEKLY
December 3, 2021

DOJ Civil Cyber-Fraud Initiative Presents New False Claims Act Challenges for Health Care Providers

Jasmine Morton, Riley Safer Holmes & Cancila LLP

Jack Theis, Riley Safer Holmes & Cancila LLP

Kelly Warner, Riley Safer Holmes & Cancila LLP

In October 2021, the Department of Justice (DOJ) announced a new Civil Cyber-Fraud Initiative as part of the government's ongoing efforts to combat cyber threats. The Initiative will use the False Claims Act (FCA) to target cybersecurity-related fraud by ensuring the technology-related representations by government contractors and grant recipients are accurate.[1]

The new Initiative follows several other announcements by the federal government that enlisted the private sector in the fight against cyber attacks. In May, President Biden signed an Executive Order on Improving the Nation's Cybersecurity calling for the federal government to partner with the private sector to protect against malicious cyber actors,[2] and in June, the White House issued a rare open letter to private sector executives recommending specific steps to enhance their cyber defenses and protect business operations.

DOJ has also joined the fray. Earlier this year, Deputy Attorney General Lisa Monaco ordered DOJ to craft specific recommendations to expand its efforts against cyber threats. The Civil Cyber-Fraud Initiative is a direct result of that review.[3]

Hospitals, nursing homes, and other health care entities receiving government funds or otherwise dealing with the federal government should take heed. As DOJ's announcement makes clear, cybersecurity is a board-level responsibility that requires the attention of senior corporate officers. In order to avoid FCA liability, health care companies that work with the federal government should review and test their cyber-related policies and procedures and take steps to ensure that sufficient technical safeguards are in place to protect their systems and data.

Details of the New DOJ Initiative

The FCA, as most health care companies that interact with the federal government know, is the government's primary civil fraud tool. The Act prohibits the knowing submission of

false or fraudulent claims for payment to the government. Penalties can be stiff and may include the imposition of corporate integrity agreements or treble damages.

According to DOJ, the Initiative announced in October 2021 will "utilize the False Claims Act to pursue cybersecurity related fraud by government contractors and grant recipients."[4] In announcing the initiative, DOJ made clear that both entities and individuals may be held liable under the Act for cyber-related fraud.

DOJ also stated that the Initiative will utilize the FCA to target three categories of activities by contractors and grantees: (1) "providing deficient cybersecurity products or services," (2) "knowingly misrepresenting their cybersecurity practices or protocols," and (3) "knowingly violating obligations to monitor and report cybersecurity incidents and breaches."[5] The second two categories are most likely to apply to health care companies and providers.

Regarding the second category, DOJ elaborated that "[m]isreporting about these practices may cause the government to choose a contractor who should not have received the contract in the first place" or "cause the government to structure a contract differently than it otherwise would have."[6] This suggests that the government may pursue a "fraud in the inducement" theory of liability under the FCA in these cases, under which the government could argue the initial fraud in procuring the contract (by misrepresenting cyber defenses) taints all future claims for reimbursement made under the contract.

For the third category, DOJ noted that government contracts often require reporting of cyber incidents that could threaten government data or systems. Under the "Basic Safeguarding" clause set forth in the Federal Acquisition Regulation (FAR), government contractors must protect their systems from cyber attacks and follow agency-specific technical requirements, many of which require prompt reporting of cyber incidents.[7] Department of Defense contactors, for example, must report cyber incidents within 72 hours.[8]

Finally, DOJ reiterated the importance of whistleblowers to combatting cyber-related fraud. Under the FCA, whistleblowers are both protected from retaliation and given the ability to initiate an FCA case on behalf of the government (and seek a portion of the recovery) through a qui tam action. In announcing the initiative, DOJ stated that whistleblowers will "play a significant role in bringing to light knowing failures and misconduct in the cyber arena," and that "whistleblower reporting will help spur compliance by contractors and grantees."[9]

Recent Cyber-Related False Claims Act Enforcement Actions

Cyber-related FCA actions are not necessarily new. In *United States ex rel. Glenn v. Cisco Systems, Inc.*,[10] for example, a whistleblower alleged that Cisco sold video surveillance

equipment to state and federal governments with significant known security flaws. Cisco ultimately settled the action in 2019 for $8.6 million.[11] In another case, *United States ex rel. Adams v. Dell Computer Corp.*,[12] a whistleblower alleged that Dell sold the government computer systems with significant undisclosed security vulnerabilities. That case was dismissed after the court found that the realtor's allegations fell short of establishing that Dell knew of the vulnerability or that the vulnerability would have altered the decision to grant the contract.[13]

But DOJ's most recent intervention in a cyber FCA case may be an indicator of things to come. In *United States ex rel. Markus v. Aerojet Rocketdyne Holdings, Inc.*,[14] a former employee of Aerojet filed a qui tam action alleging that the company had falsely certified compliance with the cybersecurity requirements within the NASA FAR and Department of Defense Federal Acquisition Regulations Supplement (DFARS).[15]

The federal government initially declined to intervene in the case, and for years, DOJ stayed on the sidelines. At the end of last month, however, the government filed a Statement of Interest in response to Aerojet's motion for summary judgment.[16] Aerojet argued that the summary judgment was warranted because causation had not been established, the non-disclosure was not material to the payment decisions, and the government was not damaged because Aerojet delivered a functional product.

In its 13-page brief, DOJ attacked each of these points, arguing that Aerojet misstated and misapplied the applicable law on causation, materiality, and damages. Notably, in rejecting the argument that the government suffered no damages, DOJ argued that Aerojet "ignores that the government did not just contract for rocket engines, but also contracted with [Aerojet] to store the government's technical data on a computer system that met certain cybersecurity requirements," and that "[f]alse claims for payment for cybersecurity services [Aerojet] failed to provide as required can be a source of damages even if the rocketry it delivered was free of defect and functioned as required."[17]

DOJ's entry into the *Aerojet* case could be seen as a precursor to how it intends to approach FCA cases involving cybersecurity in the future.

How Health Care Companies Should Respond

The announcement of the DOJ Initiative indicates a concerted effort by the federal government to investigate cyber-related fraud and use the FCA when necessary. Health care companies that interact with the government should take several concrete steps in response.

Evaluate Compliance Programs

First, in order to protect against cyber-related FCA liability, health care companies and providers should conduct a thorough review of their compliance programs, cybersecurity

policies and procedures, and reporting mechanisms. This review, which should be conducted with legal counsel to protect privilege, should include several considerations:

- Health care companies and providers should conduct periodic reviews of the company's cybersecurity obligations, including the specific obligations to the government arising out of federal statutes, regulations, or contracts, as well as any obligations placed on the company's employees and vendors.
- Because the announcement of the Initiative specifically referenced protections for whistleblowers, health care companies should ensure that sufficient internal reporting mechanisms (such as an ethics hotline) exist, and that internal policies protect reporters from retaliation.
- Statements to the government regarding a company's cybersecurity defenses and policies must be carefully vetted. This is particularly true for statements regarding the compliance with any requirements under the FAR or agency-specific supplements to the FAR. Health care companies should ensure that appropriate guidelines are in place to review all government communications.
- DOJ also specifically referenced the obligations of contractors to report cyber incidents and breaches when they occur.[18] Health care contractors and grantees should also understand the notification requirements before the incidents occur and craft incident response plans. Failure to disclose an incident or breach within the appropriate time can result in significant penalties and knowing the time frame for reporting requirements before the incident will help expedite notification decisions.

Enhance Cyber Defenses

Second, in order to ensure that cyber policies and procedures meet the appropriate technical requirements, health care companies should consult with third-party experts to assess and test their defenses. That consultation should be conducted at the direction of legal counsel and should involve the following:

- Regulatory gap assessment. This analysis will identify shortcomings in existing cybersecurity policies, processes, and procedures, helping achieve compliance through implementing necessary changes. A proper review also includes assessing the data environment and security infrastructure of the health care company, as well as how programs are implemented, managed, and enforced.
- Control development and revision strategy. This process will recommend changes regarding technology solutions, human resources, and policies centered around regulatory requirements. By first understanding the requirements listed in the DOJ Initiative, and based on the health care company's existing cybersecurity protections, a comprehensive roadmap can be developed to drive implementation, compliance, and ultimately ensure that cybersecurity practices are properly represented.
- Third-party audit and assessment. Proper cybersecurity practices or protocols extend to connected entities. Any information shared with, or network access granted to, third-party vendors can create additional vulnerabilities for exposure and provide further access points for cyber actors to leverage. A third-party due diligence assessment will analyze cyber risk of a health care company's digital ecosystem and allow for specific recommendations for how identified threats can be mitigated.

- Data breach disclosure and notification processes. Installing adequate and timely notification and reporting processes in advance will help meet compliance requirements. This includes communicating with the government and potentially law enforcement, as well as with key stakeholders and patients. Determining specifically who to contact and when, if setting up an in-bound call center is necessary, and how to notify patients—email or mailed letter—will save time and resources while in the middle of a cybersecurity incident and avoid penalties for noncompliance.

About the Authors

Jasmine Morton is an associate with Riley Safer Holmes & Cancila LLP. As a former prosecutor for the Illinois Office of the State's Attorneys Appellate Prosecutor, she focuses her practice on False Claims Act cases and government enforcement inquiries, particularly within the health care industry.

Jack Theis is a partner with Riley Safer Holmes & Cancila LLP. He draws on his experience as a former Associate White House Counsel and Department of Justice trial lawyer to counsel clients facing cybersecurity threats, government investigations, and multidimensional crises involving legal and reputational risks.

Kelly Warner is a partner with Riley Safer Holmes & Cancila LLP. She counsels clients through data and cybersecurity breaches, alleged violations of anti-kickback statutes, health care fraud, and other matters, leading internal investigations and helping them interface with the Department of Justice, Securities and Exchange Commission, Health and Human Services, and other federal and state agencies.

---

[1] Department of Justice, *Deputy Attorney General Lisa O. Monaco Announces New Civil Cyber-Fraud Initiative* (Oct. 6, 2021), https://www.justice.gov/opa/pr/deputy-attorney-general-lisa-o-monaco-announces-new-civil-cyber-fraud-initiative.

[2] Exec. Order No. 14028, 86 Fed. Reg. 26633 (May 12, 2021), https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.

[3] Department of Justice, *Deputy Attorney General Lisa O. Monaco Announces New Civil Cyber-Fraud Initiative* (Oct. 6, 2021), https://www.justice.gov/opa/pr/deputy-attorney-general-lisa-o-monaco-announces-new-civil-cyber-fraud-initiative.

[4] *Id.*

[5] *Id.*

[6] U.S. Department of Justice, *Acting Assistant Attorney General Brian M. Boynton Delivers Remarks at the Cybersecurity and Infrastructure Security Agency (CISA) Fourth Annual National Cybersecurity Summit* (Oct. 13, 2021), https://www.justice.gov/opa/speech/acting-assistant-attorney-general-brian-m-boynton-delivers-remarks-cybersecurity-and.

[7] FAR 52.204-12.

[8] Defense Federal Acquisition Regulation Supplement 204.7301-7302, https://www.acq.osd.mil/dpap/dars/dfars/html/current/204_73.htm.

[9] U.S. Department of Justice, *Acting Assistant Attorney General Brian M. Boynton Delivers Remarks at the Cybersecurity and Infrastructure Security Agency (CISA) Fourth Annual National Cybersecurity Summit* (Oct. 13, 2021), https://www.justice.gov/opa/speech/acting-assistant-attorney-general-brian-m-boynton-delivers-remarks-cybersecurity-and.

[10] No. 1:11-cv-00400 (W.D.N.Y.).

[11] N. Y. Times, *Cisco to Pay $8.6 Million to Settle Government Claims of Flawed Tech* (July 31, 2019), https://www.nytimes.com/2019/07/31/technology/cisco-tech-flaw-sales.html.

[12] No. 15-cv-608 (D.D.C.).

[13] *United States ex rel. Adams v. Dell Computer Corp*., 496 F. Supp. 3d 91, 94 (D.D.C. 2020).

[14] No. 15-cv-2245 (E.D. Cal.).

[15] First Amended Complaint, Dkt. 22, *United States ex rel. Markus v. Aerojet Rocketdyne Holdings, Inc*., No. 15-cv-2245 (E.D. Cal.).

[16] United States' Statement of Interest in Connection with Defendants' Summary Judgment Motion, Dkt. 135, *United States ex rel. Markus v. Aerojet Rocketdyne Holdings, Inc*., No. 15-cv-2245 (E.D. Cal.).

[17] *Id.* at 11.

[18] U.S. Department of Justice, *Acting Assistant Attorney General Brian M. Boynton Delivers Remarks at the Cybersecurity and Infrastructure Security Agency (CISA) Fourth Annual National Cybersecurity Summit* (Oct. 13, 2021), https://www.justice.gov/opa/speech/acting-assistant-attorney-general-brian-m-boynton-delivers-remarks-cybersecurity-and.