How To Minimize FCA Cyberfraud Enforcement Risk

By **Brenna Jenny and Sujit Raman** (November 3, 2021)

Brenna Jenny

Sujit Raman

Earlier this month, Deputy U.S. Attorney General Lisa Monaco announced the launch of the Civil Cyber-Fraud Initiative, to use the False Claims Act to pursue cybersecurity-related fraud.[1]

The U.S. Department of Justice Civil Division's acting assistant attorney general, Brian Boynton, promptly followed with a speech describing the initiative and encouraging relators to use the FCA's qui tam provision in reporting cyberfraud.[2]

Shortly thereafter, Monaco again spoke about the initiative, underscoring its importance to the DOJ's broader cybersecurity and anti-fraud efforts.[3]

Although the initiative focuses generally on government contractors and grant recipients — and does not, by its terms, impose any new cybersecurity requirements — the project promises in particular to attract whistleblowers in the defense industry, as recent years have witnessed high-profile FCA cases implicating alleged cybersecurity noncompliance in that sector.[4]

The health care industry may also see a marked increase in cybersecurity-related qui tams, especially in light of a recent report from the U.S. Department of Health and Human Services' Office of Inspector General taking the Centers for Medicare & Medicaid Services to task for failing to hold hospitals accountable for the cybersecurity of their networked devices.[5]

Health care providers and medical device manufacturers, in addition to other government contractors and grantees, would do well to heed the DOJ's warning that cybersecurity failures are prime candidates for potential False Claims Act enforcement.[6]

Government-led initiatives to improve private sector cybersecurity are nothing new. Over the years, however, these initiatives typically have encouraged industry to raise its standards voluntarily, and through dialogue with the government in a public-private partnership.

Moreover, where the procurement process was implicated, the federal government typically pushed for cybersecurity improvements in its own systems and networks, with attendant improvements to private-sector cybersecurity occurring as a byproduct.

The DOJ's new Civil Cyber-Fraud Initiative is striking because a significant uptick in investigations and enforcement actions under the FCA could sound a more adversarial tone into the traditional dynamics of threat-information sharing between industry and the federal government.

The initiative is also noteworthy because it signals the possibility that enforcement could extend in a sustained way to industry actors — including in health care — beyond those that service the federal government's own networks.

While public pronouncements about the initiative do not specifically mention the health care industry, cyberattacks on hospitals and medical devices have been on the rise.[7] The health care industry should expect that the DOJ's historical focus on health care over all other industries in the FCA context makes it more likely that this industry will be swept up into the initiative as well.

For example, hospitals may in particular wish to take steps to respond to clear frustration recently expressed by the HHS-OIG over CMS' "lack [of] consistent oversight of the cybersecurity of networked devices in hospitals."[8]

This summer, the HHS-OIG completed a review of the extent to which CMS and its contracted accrediting organizations impose and police cybersecurity standards for hospital networked devices, which include devices that monitor patient activity or obtain and communicate imaging.

The HHS-OIG noted that the conditions of participation applicable to hospitals "are silent on networked device cybersecurity as well as cybersecurity in general" and as a result, accrediting organizations "rarely use their discretion to examine the cybersecurity of networked devices during their hospital surveys."[9] The HHS-OIG advised CMS "to address cybersecurity of networked medical devices in its quality oversight of hospitals," but CMS would not commit to doing so.[10]

It is not uncommon for law enforcement to pick up the enforcement baton when they believe HHS has dropped it, and CMS' decision not to implement the HHS-OIG's recommendations may encourage the DOJ to target this area.

As Boynton noted in his recent remarks, the DOJ's new Civil Cyber-Fraud Initiative focuses on "at least three common cybersecurity failures that are prime candidates for potential False Claims Act enforcement": (1) knowing failures to comply with cybersecurity standards; (2) knowing misrepresentation of security controls and practices; and (3) the knowing failure to timely report suspected breaches.[11]

Boynton's speech repeatedly mentions that when such conduct occurs, "the government does not get what it bargained for," previewing that the DOJ plans to pursue at least some of these FCA cases using a so-called worthless-services theory of liability.

Not all courts have recognized this theory, but some have allowed relators to premise FCA claims on the notion that claims for worthless goods or services are inherently false.

However, many of these courts have emphasized that goods or services "worth less" are not "worthless" and therefore cannot, without more, sustain FCA liability.[12] Courts have underscored this distinction because, were it otherwise, the FCA would become a vehicle for "punishing garden-variety breaches of contract or regulatory violations" — which the U.S. Supreme Court has clearly prohibited.[13]

The theory that items or services with cybersecurity flaws are worthless would be novel. And even if certain cybersecurity flaws could render items or services worthless, the proverbial line in the sand separating what is "worth less" from what is "worthless" remains ill-defined.[14]

Some courts that considered the worthless-services theory concluded that items or services become worthless when provided with gross negligence, i.e., a lack of even slight diligence or care, whereas ordinary negligence falls short of the worthless standard.[15]

In all events, as with many FCA theories of liability, this one may evolve and proliferate primarily through DOJ settlements with defendants that cannot risk the financial ruin that would come from a litigation loss under the FCA, which could include treble damages, statutory penalties and possible exclusion or debarment.

The DOJ's encouragement to relators has been picked up by the whistleblowers' bar, which is already encouraging cybersecurity whistleblowers to come forward.[16] The initiative thus serves as a strong reminder to those selling items or services to the federal government, as well as to those who solicit and receive federal grants, that they should take steps now to incorporate rigorous cybersecurity safeguards that could serve as a defense to an FCA theory of liability, should a cyber incident take place.

Government contractors, grant recipients, health care providers and medical device manufacturers wishing to minimize their exposure under the FCA — and the DOJ initiative — should consider the following preventative steps, as applicable.

Update cybersecurity and information security policies to ensure they align with best practices.

What the best practices are can be unclear, as different agencies may have different standards, and as the federal government — through President Joe Biden's May 2021 "Executive Order On Improving the Nation's Cybersecurity" — itself has announced a review of those standards.

Nonetheless, the executive order already has imposed new cybersecurity standards on certain government contractors that could end up being the subject of whistleblowing and qui tam suits. These entities should ensure they are up-to-date on the relevant standards, and should avoid getting even close to the line of making any false certifications.

Review contractual terms for ambiguities or lack of clarity, as well as for diversity of requirements.

Different federal agencies often have their own contract cyber clauses, and different contracts within the same agency may have different obligations. Companies should assess their government contracts, evaluate what their cybersecurity obligations are and conduct a risk assessment that identifies where attention should be focused.

Monitor enforcement actions and court decisions to ensure that companies are aware of ongoing trends, and of what may constitute material noncompliance with cybersecurity rules and regulations for FCA purposes.

A 2015 case, U.S. v. NetCracker Technology Corp., in the U.S. District Court for the District of Columbia provides a cautionary example.

The Netcracker settlement, which resolved allegations that a company used employees without security clearances on certain U.S. Department of Defense projects in violation of express contract requirements, may indicate that the DOJ could extend the initiative's scope to cover cases involving not only core cybersecurity issues, but also data protection issues involving personnel without security clearances, or non-U.S. citizen employees, where contracts require otherwise.[17]

As enforcement actions and court cases on this issue possibly evolve to encompass a

worthless-services theory, understanding how the government is defining "worthless" will also be important.

Ensure incident response plans are up-to-date and tested.

Monaco pointed out that entities or individuals who knowingly violate obligations to monitor and report cybersecurity incidents and breaches may draw FCA scrutiny. It is important to ensure that compliance personnel are aware of the company's statutory, regulatory, contractual and grant-based obligations, and execute them accordingly.

Align outward messaging about cybersecurity capabilities.

Companies should confirm that marketing personnel and procurement specialists closely coordinate with more technical personnel, so that outward-facing communications about cybersecurity capabilities remain clear, consistent and accurate.

Brenna E. Jenny and Sujit Raman are partners at Sidley Austin LLP.

[1] Press Release, 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] Remarks of Acting Assistant Attorney General Brian M. Boynton 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. Earlier, in December 2020, Civil Division leadership had signaled that "cybersecurity related fraud is another area where we could see enhanced False Claims Act activity." See Remarks of Deputy Assistant Attorney General Michael D. Granston at the ABA Civil False Claims Act and Qui Tam Enforcement Institute (Dec. 2, 2020), https://www.justice.gov/opa/speech/remarks-deputy-assistant-attorney-general-michael-d-granston-aba-civil-false-claims-act.

[3] Remarks of Deputy Attorney General Lisa O. Monaco and Assistant Attorney General Kenneth A. Polite, Jr. at the Criminal Division's Cybersecurity Roundtable on 'The Evolving Cyber Threat Landscape' (Oct. 20, 2021), https://www.justice.gov/opa/speech/deputy-attorney-general-lisa-o-monaco-and-assistant-attorney-general-kenneth-polite-jr.

[4] See, e.g., United States ex rel. Markus v. Aerojet Rocketdyne Holdings, Inc., and Aerojet Rocketdyne, Inc. , No. 2:15-cv-02245 (E.D. Cal. May 8, 2019) (allegation that company violated the FCA by submitting and conspiring to submit false certifications that it was compliant with cybersecurity requirements found in federal contracts); see also United States ex rel. Glenn v. Cisco Systems, Inc., No. 1:11-cv-00400-RJA (W.D.N.Y. 2019) (allegation that one of company's products failed to comply with government customer cybersecurity requirements); United States ex rel. Kingsley v. NetCracker Technology Corp., No. 1:11-cv-00629 (D.D.C. 2015) (allegation that telecom software and services company used individuals without security clearances in violation of a Defense Information Systems

Agency contract).

[5] HHS-OIG, Medicare Lacks Consistent Oversight of Cybersecurity for Networked Medical Devices in Hospitals (June 2021) [hereinafter OIG Networked Devices Report], https://oig.hhs.gov/oei/reports/OEI-01-20-00220.pdf.

[6] https://www.justice.gov/opa/speech/acting-assistant-attorney-general-brian-m-boynton-delivers-remarks-cybersecurity-and.

[7] See, e.g., Heather Landi, Fierce Healthcare, Relentless cyberattacks are putting financial pressure on hospitals: Fitch Ratings (July 26, 2021), https://www.fiercehealthcare.com/tech/relentless-cyber-attacks-are-putting-pressure-hospital-finances-fitch-ratings.

[8] OIG Networked Devices Report at 12.

[9] Id.

[10] Id.at 12, 15.

[11] Remarks of Acting Assistant Attorney General Brian M. Boynton 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.

[12] See, e.g., United States ex rel. Absher v. Momence Meadows Nursing Center, Inc. , 764 F.3d 699 (7th Cir. 2014).

[13] Universal Health Servs., Inc. v. United States ex rel. Escobar , 579 U.S. 176, 136 S. Ct. 1989, 2003 (2016).

[14] See, e.g., United States ex rel. Jackson v. DePaul Health Sys. , 454 F. Supp. 3d 481, 496 (E.D. Pa. 2020) (quoting United States v. Houser, 754 F.3d 1335, 1344 (11th Cir. 2014)).

[15] Id.

[16] See, e.g., Tycko & Zavareei Whistleblower Practice Group, Calling all Cybersecurity Whistleblowers: DOJ Wants You to Report Cyber Fraud (Oct. 13, 2021), https://www.natlawreview.com/article/calling-all-cybersecurity-whistleblowers-doj-wants-you-to-report-cyber-fraud.

[17] U.S. ex rel. Kingsley v. NetCracker Technology Corp. No. 11-cv-00629 (D.D.C.), resolved on Oct. 27, 2015, https://www.justice.gov/opa/pr/netcracker-technology-corp-and-computer-sciences-corp-agree-settle-civil-false-claims-act.