GIBSON DUNN

October 16, 2023

FALSE CLAIMS ACT RISKS FOR CYBER DEVICE MANUFACTURERS ARISING UNDER NEW REQUIREMENTS SUBJECT TO FDA ENFORCEMENT BEGINNING OCTOBER 1, 2023

To Our Clients and Friends:

The False Claims Act (FCA) is one of the government's chief tools to address false claims involving government funds, imposing liability on "any person who… knowingly presents, or causes to be presented, a false or fraudulent claim for payment" to the federal government or who "knowingly makes, uses, or causes to be made or used, a false record or statement material to a false or fraudulent claim."[1] Through its *qui tam* provisions, the FCA also allows private citizens to file suit on behalf of the government for statutory violations.[2]

The FCA has been increasingly used to address cybersecurity concerns for companies receiving government reimbursement. In October 2021, the DOJ announced its Civil Cyber-Fraud Initiative (the Initiative), emphasizing its intent to use the FCA to hold accountable entities that knowingly (1) provide deficient cybersecurity products or services, (2) misrepresent their cybersecurity practices or protocols, or (3) violate obligations to monitor and report cybersecurity incidents and breaches.[3] Since announcing the Initiative, the DOJ has acted on its commitment by introducing a range of new cybersecurity obligations in government contracts and pursuing various investigations into whether companies have made false statements regarding their cybersecurity compliance.

Digital health companies and drug and device makers are no exception. Recent cases and investigations have been brought against digital health companies and manufacturers of "cyber devices" whose products are directly or indirectly reimbursed by the government. Accordingly, digital health and cyber device companies need to be diligent regarding their cybersecurity systems and claims.

In light of recent enforcement trends, in this alert we discuss:

- Recent Federal Food, Drug, and Cosmetic Act (FDCA) amendments requiring cybersecurity information in premarket submissions for cyber devices, as well as the potential implications for FCA liability, and

- The rise of FCA cases for claims relating to cybersecurity in the healthcare industry more generally.

Cyber Devices and False Claims in the FDA Approval Process

Recent developments have expanded the risk of cybersecurity-related FCA claims against companies making submissions to the FDA for premarket approval or clearance of cyber devices. On December 29,

2022, the Consolidated Appropriations Act, 2022 (CAA), amended the FDCA to add section 524B, which requires that premarket submissions for cyber devices contain cybersecurity information, including the company's plans to address cybersecurity vulnerabilities, processes to provide a reasonable assurance that the devices are cybersecure, a software bill of materials, and other information as the Secretary requires.[4] Under the new regulations, cyber devices are defined as any device that: (1) includes software validated, installed or authorized by the sponsor as a device or in a device; (2) has the ability to connect to the internet; and (3) contains any technological characteristics validated, installed, or authorized by the sponsor that could be vulnerable to cybersecurity threats.[5] FDCA section 524B became effective on March 29, 2023, 90 days after enactment of the CAA.[6] However, FDA announced a seven-month transition period of enforcement discretion during which FDA offered support to applicants to navigate the cybersecurity requirements.[7] FDA has stated that, as of October 1, 2023, it expects companies will have had sufficient time to adapt and comply with the new cybersecurity requirements.[8]

More extensive cybersecurity disclosures to FDA expand the potential for cybersecurity-related false statements and subsequent FCA risk. FCA cases for false statements to FDA rely on the "fraud-on-the-FDA" theory. Under the theory, a company may be liable under the FCA if false statements to FDA are material to FDA's approval or clearance of the device, rendering later claims to a governmental entity, such as the Centers for Medicaid and Medicare Services, false.

The "fraud-on-the FDA" theory was rejected by the First Circuit in *D'Agostino v. EV3, Inc*., in 2016.[9] In that case, the court held that there was no causal link between false representations to FDA and subsequent payments by the Centers for Medicare and Medicaid Services (CMS).[10] However, since *D'Agostino*, cases in the Ninth Circuit and statements from the DOJ have suggested that the possibility of FCA liability based on false statements to FDA is not null.

In cases in 2017 and 2021, the Ninth Circuit allowed two FCA cases to go forward in cases where it found that 1) alleged false claims made FDA clearances or approvals fraudulent in the first instance, rendering the subsequent payments to be false, or 2) the false claims rendered the drug at issue not approved or cleared for any proper purpose, making the subsequent claims for payment false.[11] Following the Ninth Circuit's decisions, the DOJ also filed a statement of interest in *U.S. ex rel. Crocano v. Trividia,* expressing its stance that "[compliance with the] FDCA may, in certain circumstances, be material to the government's decision whether to pay for the affected product, and thus relevant in an FCA case." [12] The Statement explains that per the DOJ's understanding of the FCA, FDCA violations may be relevant where the violations are "significant, substantial, and give rise to actual discrepancies in the composition, function, safety, or efficacy of the affected product," such that the product's "quality, safety, and efficacy fell below what was specified to by the Food and Drug Administration through its approval process." [13] The Second Circuit ultimately dismissed the case in *Trividia*, but left open the possibility that fraudulent statements to the FDA could result in FDA liability.[14]

While the courts have made it clear that there must be a very high showing of materiality between the false statement to FDA, FDA clearance or approval, and subsequent government payments, the possibility of FCA liability for false statements during the FDA approval process has not been entirely

foreclosed. If a company's false or fraudulent statement in a premarket submission to FDA regarding a company's cybersecurity system is material to FDA's approval of the device, such that in light of the misstatement, the "quality, safety, and efficacy of the device fell below what was specified to by the Food and Drug Administration through its approval process," the statement may draw the attention of the government and FCA plaintiffs. Similarly, false or fraudulent statements in a premarket notification could be material to clearance of a 510(k) device. Information such as companies' plans to address cybersecurity vulnerabilities, which are specifically required under the new statutory provision, and which FDA has stressed in guidance are critical to patient safety, may be considered material for the purposes of FCA claims.[15]

With this increased focus on cybersecurity for FCA investigations and the potential reopening of the fraud-on-the-FDA theory of liability, companies should take significant care in the statements made to FDA regarding their cybersecurity practices and procedures.

Cybersecurity-Related FCA Claims Since the Civil Cyber-Fraud Initiative

FCA claims involving cyber devices would fall readily into the line of enforcement actions brought against other companies for false claims relating to cybersecurity systems and disclosures. Prior to the launch of the Initiative, in *U.S. ex rel. Delaney v. eClinicalWorks*, eClinicalWorks, one of the largest vendors of electronic health records software, agreed to pay $155 million to resolve claims that it had allegedly misrepresented the security capabilities of its software as part of the certification process for the Department of Health and Human Services' Electronic Health Records Incentive Program.[16] In *U.S. ex rel. Awad v. Coffey Health System*, the hospital system, Coffey Health, agreed to pay $250,000 to settle claims alleging that it falsely attested that it had conducted security risk analyses as part of the same Electronic Health Records Incentive Program.[17]

In the DOJ's first resolution under the Initiative, *United States ex rel. Lawler v. Comprehensive Health Servs., Inc. et al.* and *United States ex rel. Watkins et al. v. CHS Middle East, LLC*, global medical services provider Comprehensive Health Services LLC agreed to pay $930,000 to settle claims that it allegedly failed to comply with contract requirements for medical services, including the use of a secure electronic medical records system.[18] More recent cases, such as a June 2023 settlement by Jelly Bean Communications Design LLC for alleged failures to maintain the ongoing cybersecurity of a health insurance website, suggest that the DOJ's spotlight on cybersecurity and healthcare companies only stands to grow.[19]

Takeaways

Cybersecurity is a major focus area for government FCA investigations. In light of recent new cybersecurity requirements, content in premarket submissions to FDA on cybersecurity procedures and disclosures constitute another area of increasing risk for companies. It is critical for companies with products or services that may receive government reimbursement to ensure that their cybersecurity systems are up-to-date and any statements made regarding those systems are accurate. Doing so will be central to managing FCA risk in the rapidly-changing cybersecurity landscape.

[1] False Claims Act (FCA), 31 U.S.C. § 3729(a)(1)(A)–(B).

[2] *Id.* at § 3730(c)-(d).

[3] U.S. Dep't of Justice, Press Release, "Deputy Attorney General Lisa O. Monaco Announces New Civil Cyber-Fraud Initiative" (Oct. 6, 2021).

[4] *See* U.S. Food & Drug Admin., "Cybersecurity in Medical Devices: Frequently Asked Questions" (Sept. 26, 2023).

[5] 21 U.S.C. § 360n-2(c); *see also* U.S. Food & Drug Admin., "Cybersecurity in Medical Devices: Frequently Asked Questions" (Sept. 26, 2023). A "device" is more generally defined by FDCA section 201(h) as an instrument, apparatus, implement, machine, contrivance, implant, in vitro reagent, or other similar or related article, including a component part, or accessory which is: (A) recognized in the official National Formulary, or the United States Pharmacopoeia, or any supplement to them; (B) intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease, in man or other animals, or (C) intended to affect the structure or any function of the body of man or other animals, and which does not achieve its primary intended purposes through chemical action within or on the body of man or other animals and which is not dependent upon being metabolized for the achievement of its primary intended purposes. The term "device" does not include software functions excluded pursuant to section 520(o). Food, Drug & Cosmetic Act, section 201(h); U.S. Food & Drug Admin., "How to Determine if Your Product is a Medical Device" (March 29, 2022).

[6] CAA § 3305(c), 21 U.S.C. § 331 note.

[7] U.S. Food & Drug Admin., "Cybersecurity in Medical Devices: Frequently Asked Questions" (Sept. 26, 2023); 88 Fed. Reg. 19148 (Mar. 30, 2023).

[8] U.S. Food & Drug Admin., "Cybersecurity in Medical Devices: Frequently Asked Questions" (Sept. 26, 2023); 88 Fed. Reg. at 19149.

[9] *D'Agostino v. EV3, Inc.*, 845 F.3d 1 (1st Cir. 2016).

[10] *Id.*, at 7.

[11] *Dan Abrams Co. v. Medtronic Inc.*, No. 19-56377 (9th Cir. 2021); *US ex rel. Campie v. Gilead Sciences, Inc.*, 862 F. 3d 890 (9th Cir. 2017).

[12] U.S. Statement of Interest in *U.S. ex rel. v. Trividia Health Inc.*, CASE NO. 22-CV-60160-RAR (S.D. Fla.).

[13] *Id.*, at 2.

[14] *United States of America ex rel., Patricia Crocano v. Trividia Health Inc.,* Order Granting Mot. to Dismiss (S.D. Fla. 2022).

[15] 21 U.S.C. § 360n-2(b)(1); U.S. Food & Drug Admin., Guidance for Industry and Food & Drug Admin. Staff, Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions (Sept. 27, 2023), at 11.

[16] U.S. Dep't of Justice, Press Release, "Electronic Health Records Vendor to Pay $155 Million to Settle False Claims Act Allegations" (May 31, 2017).

[17] U.S. Dep't of Justice, Press Release, "Kansas Hospital Agrees to Pay $250,000 To Settle False Claims Act Allegations" (May 31, 2019).

[18] U.S. Dep't of Justice, Press Release, "Medical Services Contractor Pays $930,000 to Settle False Claims Act Allegations Relating to Medical Services Contracts at State Department and Air Force Facilities in Iraq and Afghanistan" (March 8, 2022).

[19] U.S. Dep't of Justice, Press Release, "Jelly Bean Communications Design and its Manager Settle False Claims Act Liability for Cybersecurity Failures on Florida Medicaid Enrollment Website" (March 14, 2023).

*The following Gibson Dunn lawyers assisted in preparing this alert: Winston Chan, Jonathan Phillips, Gustav Eyler, John Partridge, Christopher Rosina, Carlo Felizardo, and Nicole Waddick.**

Gibson Dunn lawyers regularly counsel clients on the False Claims Act issues. Please feel free to contact the Gibson Dunn lawyer with whom you usually work, the authors, or any leader or member of the firm's False Claims Act/Qui Tam Defense Group:

False Claims Act/Qui Tam Defense Group:

Washington, D.C.
Jonathan M. Phillips – Co-Chair (+1 202-887-3546, jphillips@gibsondunn.com)
F. Joseph Warin (+1 202-887-3609, fwarin@gibsondunn.com)
Joseph D. West (+1 202-955-8658, jwest@gibsondunn.com)
Geoffrey M. Sigler (+1 202-887-3752, gsigler@gibsondunn.com)
Lindsay M. Paulin (+1 202-887-3701, lpaulin@gibsondunn.com)
Gustav W. Eyler (+1 202-955-8610, geyler@gibsondunn.com)

San Francisco
Winston Y. Chan – Co-Chair (+1 415-393-8362, wchan@gibsondunn.com)
Charles J. Stevens (+1 415-393-8391, cstevens@gibsondunn.com)

New York
Reed Brodsky (+1 212-351-5334, rbrodsky@gibsondunn.com)
Mylan Denerstein (+1 212-351-3850, mdenerstein@gibsondunn.com)
Alexander H. Southwell (+1 212-351-3981, asouthwell@gibsondunn.com)
Christopher Rosina – New York (+1 212-351-3855, crosina@gibsondunn.com)
Brendan Stewart (+1 212-351-6393, bstewart@gibsondunn.com)

Denver
John D.W. Partridge (+1 303-298-5931, jpartridge@gibsondunn.com)
Robert C. Blume (+1 303-298-5758, rblume@gibsondunn.com)
Monica K. Loseman (+1 303-298-5784, mloseman@gibsondunn.com)
Ryan T. Bergsieker (+1 303-298-5774, rbergsieker@gibsondunn.com)

Dallas
Andrew LeGrand (+1 214-698-3405, alegrand@gibsondunn.com)

Los Angeles
Nicola T. Hanna (+1 213-229-7269, nhanna@gibsondunn.com)
Jeremy S. Smith (+1 213-229-7973, jssmith@gibsondunn.com)
Deborah L. Stein (+1 213-229-7164, dstein@gibsondunn.com)
James L. Zelenay Jr. (+1 213-229-7449, jzelenay@gibsondunn.com)

Palo Alto
Benjamin Wagner (+1 650-849-5395, bwagner@gibsondunn.com)

**Nicole Waddick is an associate practicing in the firm's San Francisco office who currently is not admitted to practice law.*