PG Briefing
October 31, 2024

Three Years of the DOJ's Civil Cyber-Fraud Initiative: Examining the Government's Lawsuit Against Georgia Tech and its Implications for the Health Care Industry

David A. O'Neal (Parker Hudson Rainer & Dobbs LLP)
Travis C. Williams (Parker Hudson Rainer & Dobbs LLP)

This article is brought to you by AHLA's Fraud and Abuse Practice Group.

The number of cyberattacks has exploded in recent years, and the health care industry has borne the brunt of them. According to the World Economic Forum, the health care industry suffered 14.2% of the cyberattacks targeting critical infrastructure from January 2023 through April 2024—more than any other sector during that period.[1] This figure includes the headline-grabbing Change Healthcare ransomware attack in 2024, which perhaps best exemplifies the growing cost of cyberattacks in the health care sector.[2] In addition to the operational disruptions, loss of patient or customer trust, and private litigation that can stem from cyber incidents, health care companies also face an increase in cybersecurity-related enforcement by the Department of Justice (DOJ), including False Claims Act (FCA) cases brought as part of the DOJ's Civil Cyber-Fraud Initiative.[3]

Three years into the initiative, the DOJ is picking up steam. In August, the government intervened in an FCA lawsuit against Georgia Tech Research Corporation (GTRC) and the Board of Regents of the University System of Georgia (collectively, Georgia Tech). The Georgia Tech case is the first FCA case under the Civil Cyber-Fraud Initiative (CCFI) in which the DOJ has intervened. This case, as well as other cyber-fraud settlements by the DOJ, make clear that cyber-fraud enforcement remains a top priority for the DOJ, and that companies may come under scrutiny regardless of whether there is a data breach.

The DOJ's Civil Cyber-Fraud Initiative

Deputy Attorney General Lisa O. Monaco announced the Civil Cyber-Fraud Initiative in October 2021.[4] The DOJ conceived of the initiative to "utilize the False Claims Act to pursue cybersecurity related fraud by government contractors and grant recipients."[5] Specifically, Deputy Attorney General Monaco stated that the DOJ would target individuals and companies who are (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."[6] The first two years of the initiative were relatively slow as relators and the government began filing and investigating cyber-related qui tam actions. Only two cases were announced as part of the initiative in 2022 and 2023.

Comprehensive Health Services

In March 2022, the DOJ announced the first settlement under the initiative with Comprehensive Health Services LLC (CHS), a provider of global medical services that contracted with the federal government to provide medical services at government-run facilities in Iraq and Afghanistan.[7] CHS paid $930,000 to resolve allegations that it violated the FCA by submitting claims to the State Department for the cost of a secure electronic medical record system to store patients' medical records, which it allegedly failed to use consistently.[8] The complaint alleged that CHS staff left copies of scanned medical records on an internal network drive accessible by non-clinical staff, and when staff members raised this privacy concern, CHS did not take adequate remedial steps.[9] U.S. Attorney Breon Peace said that "[the] settlement serves notice to federal contractors that they will be held accountable for conduct that puts private medical records and patient safety at risk."[10]

Jelly Bean Communications Design LLC

One year later, the DOJ announced a settlement with defendants Jelly Bean Communications Design LLC (Jelly Bean) and its sole employee and manager.[11] Jelly Bean contracted with the Florida Healthy Kids Corporation (FHKC), a state-created entity that receives federal Medicaid funds, to provide "website design, programming and hosting services" for a website through which parents could apply for Medicaid coverage for their children.[12] The contract provided that Jelly Bean would provide a fully functional hosting environment that complied with the Health Insurance Portability and Accountability Act of 1996 (HIPAA).[13] Around early December 2020, it became clear that over 500,000 applications, along with applicants' personal information, had been hacked and altered.[14] In response to the breach, FHKC shut down the application portal.[15] The defendants settled for $293,771.[16]

The Initiative Picks up Steam in 2024

In 2024, the CCFI appears to be hitting its stride. In addition to the intervention against Georgia Tech and the settlement with Penn State discussed below, the DOJ has announced three multi-million-dollar settlements—one in April and two in May.[17]

Insight Global LLC

In April 2024, the DOJ announced that Insight Global LLC had settled FCA allegations for $2.7 million, the largest health care-related CCFI settlement to date.[18] The Atlanta-headquartered firm contracted with the Pennsylvania Department of Health to provide staffing for COVID-19 contact tracing.[19] In Statements of Work submitted under the contract, Insight Global represented that it "recognizes and accepts that the contact tracing workforce will have access to personal health information of contact tracing subjects and must ensure that and all other such information related to the services being provided must be kept confidential and secure."[20] Despite this representation, Insight Global staff allegedly engaged in unsecure practices with personal health information such as transmitting it through unencrypted emails, accessing it using shared passwords, and storing and transmitting it using Google files that were not password protected and were potentially accessible to the public.[21] Furthermore, Insight Global allegedly received complaints from staff about these practices from November 2020 to January 2021 but failed to begin remediation efforts until April 2021.[22]

Guidehouse and Nan McKay and Associates

The two May 2024 CCFI settlements involved non-health care defendants Guidehouse, Inc. and Nan McKay and Associates (NMA), both government contractors that were tasked with implementing a website where low-income New Yorkers could apply for federal rental assistance during the COVID-19 pandemic.[23] Both defendants allegedly failed to complete the pre-production cybersecurity testing that their government contracts required, and within 12 hours of the website's launch, a New York state agency shut it down because applicants' personally

identifiable information had been compromised and leaked on the internet.[24] Guidehouse and NMA settled with DOJ for $7.6 million and $3.7 million, respectively.[25]

The Government's Lawsuit Against Georgia Tech: ***United States ex rel. Craig v. Georgia Tech Research Corporation***

The Complaint

Despite the increasing number of settlements, the DOJ had yet to intervene and litigate an FCA case under the Civil Cyber-Fraud Initiative. That changed in August 2024 when the government filed its complaint in intervention in a qui tam action filed against Georgia Tech. The case was initially filed in August 2022 by two Georgia Tech cybersecurity professionals, including its current Associate Director of Cyber Security. The government's complaint-in-intervention was filed just over two years later—a relatively swift investigation and intervention by DOJ standards—and significantly expanded the qui tam relators' allegations. The government's 99-page complaint-in-intervention is roughly three times longer than the complaint filed by the whistleblowers.[26]

The complaint alleges claims under the FCA against GTRC only, as well as common law claims for fraud, negligent misrepresentation, unjust enrichment, and payment by mistake against both GTRC and Georgia Tech. The government's claims are based upon Georgia Tech's alleged violation of Department of Defense (DoD) regulatory and contractual obligations to provide "adequate security" on their information systems.[27] As a condition of entering DoD contracts, federal regulations require DoD contractors to implement and certify their compliance with certain cybersecurity standards, particularly the 110 controls set forth in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171.[28]

The DOJ alleged that Georgia Tech knowingly violated these NIST SP 800-171 requirements for Astrolavos Lab, which conducted research for DoD that, ironically enough, was focused on cybersecurity.[29] Specifically, the government alleged that Georgia Tech failed to "develop, document, implement, and periodically update system security plans and associated NIST SP 800-171 security controls" at Astrolavos Lab.[30] Despite being purportedly required to do so by regulation after December 31, 2017, the DOJ alleged that Astrolavos Lab had no security plan at all until February 2020.[31] And when the lab did implement a security plan, the complaint alleged that Astrolavos Lab inappropriately excluded from its plan most of the desktop and laptop computers within the lab.[32]

The complaint-in-intervention next alleged that Georgia Tech failed "install, update, and run antivirus and incident detection software" at Astrolavos Lab.[33] Executive leadership allegedly pressured the compliance team at Georgia Tech to allow the Astrolavos Lab not to run anti-virus software, based off of complaints by the lab director, who the complaint described as a "star quarterback" who used his power on campus to shirk cybersecurity requirements.[34]

The government also alleged that Georgia Tech provided DoD with a false summary level score in order to obtain and retain DoD contracts.[35] Federal regulations require that contractors provide the DoD a report of the status of their compliance with the 110 controls set forth in NIST SP 800-171.[36] According to the government's complaint, Georgia Tech submitted a report to the DoD that falsely suggested that Georgia Tech had a campus-wide IT system when, in reality, no such plan existed.[37] The compliance team, the government alleged, was instructed by the department that oversees government contracting at Georgia Tech to submit a campus-wide summary level score.[38] The compliance team, therefore, created a campus-wide system security plan and gave Georgia Tech a score of 98 out of 110.[39] But the security plan was only a "model" according to the DOJ, and the drafter of the campus-wide plan admitted in sworn testimony that the score of 98 was not actually earned by a Georgia Tech IT system.[40]

In addition to FCA violations, the DOJ complaint alleges claims for common law fraud,[41] negligent misrepresentation,[42] unjust enrichment,[43] payment by mistake,[44] and breach of contract.[45] Georgia Tech's lawyers have indicated in a court filing that they will be moving to dismiss the government's complaint-in-intervention.

Georgia Tech's Motion to Dismiss

On October 21, Georgia Tech moved to dismiss the Government's complaint, arguing that the government failed to plead viable FCA or common law claims.[46] A few of those arguments are particularly noteworthy. For example, Georgia Tech claimed that the contracts at issue were for "fundamental research," which is completely exempted from the DoD cybersecurity regulations that underpinned the DOJ's claims.[47] Such research is "basic and applied research in science and engineering, the results of which are published and shared broadly within the scientific community."[48] Georgia Tech also argued that, even if the DoD cybersecurity regulations applied to the Astrolavos Lab, the Complaint inappropriately attempts to hold GTRC responsible for failing to comply with the wrong version of the NIST controls, which went into effect after one of the relevant contracts were executed.[49]

Georgia Tech also moved to dismiss on the grounds that the government failed to allege that the alleged cybersecurity violations were material to the DoD's decision to pay.[50] Georgia Tech claimed that the DoD cybersecurity controls did not go to the essence of the government's bargain.[51] Georgia Tech points out that those regulations require a DoD contracting officer to verify Georgia Tech's summary level score, and yet the complaint fails to allege that anyone actually did so.[52] What's more, Georgia Tech claims that DoD knew about the alleged violations no later than July 2022 when the qui tam complaint was filed, and continued to pay GTRC $10 million after that time.[53]

Interestingly, although the argument was not fully developed, Georgia Tech preserved an argument that the qui tam provisions of the FCA are unconstitutional, in light of the recent Middle District of Florida decision in *United States ex rel. Zafirov*, which held that the qui tam provisions violate the Appointments Clause of the Constitution.[54]

What to Watch in the Georgia Tech Case

Although Georgia Tech's motion to dismiss arguments have the potential to be fatal for the government's case, many of them may be premature. Georgia Tech relies upon numerous documents not referenced in the complaint in support of several of its arguments, including the argument that GTRC was performing "fundamental research" and has asked the court to take judicial notice of these documents.[55] The court may be reluctant to do so at the motion to dismiss stage and instead entertain such arguments at summary judgment.

In the event that Georgia Tech loses its motion to dismiss, discovery may present a host of challenges for the government, particularly on the issue of materiality. Georgia Tech would be entitled to discovery not only on the DoD's decision to continue making payments to GTRC in the wake of learning about the supposed cybersecurity violations, but also the DoD's actions with respect to other contractors with similar violations throughout the country. Georgia Tech may even attempt to take discovery of the government's own cybersecurity failures, which may be relevant to Georgia Tech's defenses for the equitable claims brought by the DOJ.

A win by Georgia Tech on its motion to dismiss or at summary judgment has the potential to undermine the message that DOJ is attempting to send with the Civil Cyber-Fraud Initiative. The government may, therefore, attempt to settle the case on terms that both sides can live with. Indeed, on October 22, 2024, the day after Georgia Tech filed its motion to dismiss, Pennsylvania State University (Penn State) settled a similar FCA matter for $1,250,000.[56] Like the Georgia Tech case, the Penn State settlement was also based on allegations that the university failed to implement controls under NIST SP 800-171, as required by a DoD contract, for a period of more than five years.[57] The government may, however, view the Georgia Tech case as more significant and

egregious than the Penn State case, given that the DOJ failed to reach a similar settlement with Georgia Tech prior to intervention.

Takeaways for the Health Care Industry

The DOJ is Not Waiting for a Cyber Incident to Bring Cases Under the FCA

Many of the CCFI cases—including the cases against Georgia Tech, Penn State, Insight Global, and CHS—did not arise out of data breach events. The DOJ is using the initiative to send a strong message to companies who do business with the government that they must be proactive in implementing cybersecurity measures. Health care companies must take a close look at what contractual promises they have made regarding cybersecurity and document the steps they have taken to comply with them. Simply having a clean track record is not sufficient to avoid DOJ scrutiny.

Make Sure Your Organization Has Team Players, Not Star Quarterbacks, When It Comes to Cybersecurity

One of the key allegations in the DOJ's complaint against Georgia Tech was that "star quarterback" researchers were able to push back on or ignore the cybersecurity compliance requirements in DoD contracts "because they found it burdensome."[58] The government alleges that senior leadership gave in to the demands of these researchers because of the money they generated from government contracts.[59] It remains to be determined whether the government's allegations are factual, but the compliance point remains. Companies must build a culture of compliance that comes from the top down and in which everyone is vested in doing their part to implement cybersecurity measures.

A Strong Compliance Culture Reduces the Risk of Whistleblowers

The whistleblowers in both the Georgia Tech and Penn State cases were members of the universities' cybersecurity teams who apparently felt that their concerns about cybersecurity compliance with DoD were not being heard. Cybersecurity professionals are often asked to do much within an organization, especially given the increasingly onerous standards required of government contracts. Organizations must support and value the input of these individuals, particularly when they raise compliance concerns.

The Civil Cyber-Fraud Initiative Has Focused on Specific Contractual Cybersecurity Requirements, but Broader Enforcement is Possible

To date, the Civil Cyber-Fraud Initiative has involved claims submitted under government contracts that either directly impose or are conditioned upon contractual certifications of compliance with a specific set of cybersecurity requirements. Other than the Jelly Bean settlement with a website host, DOJ has yet to bring or settle a case premised upon HIPAA violations. But there is some recent authority suggesting that violations failure to comply with HIPAA's security rule may provide a foothold into the FCA.

In December 2022, a federal court in Georgia held that relators adequately alleged FCA claims against eClinicalWorks, LLC (eClinicalWorks), an electronic health record (EHR) software developer.[60] Among other arguments made by the relators was eClinicalWorks' EHR software also cased health care providers to impliedly certify their compliance with the HIPAA security regulations when they submit a claim for payment to CMS or one of CMS' contractors."[61] Despite the court's explicit skepticism of the relators' HIPAA certification theory, which it emphasized by noting "a near total dearth of authority suggesting that the arguably vague HIPAA Security Rule can be the basis for an FCA claim," the court allowed the claims to proceed.[62]

Another court in Illinois made a similar ruling, allowing relators' claims to proceed based on HIPAA violations, and the case was subsequently settled for an undisclosed sum.[63] Despite the acknowledged lack of cases, the court found that it could "analogize to other FCA cases": if paying kickbacks to solicit patients had a "good probability" of affecting a payment decision, then HIPAA-based FCA claims were also viable.[64]

Although DOJ has not yet brought or intervened in FCA cases premised on HIPAA violations, the acceleration of Civil Cyber-Fraud Initiative indicates that the agency increasingly sees the FCA as a tool for addressing cyberattacks and deterring lax cybersecurity practices. And even without the DOJ's involvement in these types of cases, the judicial approval of such theories creates significant risk that health care providers might be required to defend such actions. Health care providers should be careful to account for the cybersecurity risks posed not only within their own organizations but also by third-party vendors, particularly those with direct access to EHRs.

---

[1] Akshay Joshi, *These Sectors Are Top Targets for Cybercrime, and Other Cybersecurity News to Know This Month*, WORLD ECON. F. (Apr. 22, 2024), https://www.weforum.org/agenda/2024/04/cybercrime-target-sectors-cybersecurity-news/.
[2] Bruce Japsen, *UnitedHealth Group Cyberattack Costs to Hit $2.3 Billion This Year*, FORBES (July 16, 2024), https://www.forbes.com/sites/brucejapsen/2024/07/16/unitedhealth-group-cyberattack-costs-to-eclipse-23-billion-this-year/.
[3] Press Release, Off. of Pub. Affs., U.S. Dep't of Just., 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] *Id.*
[7] Press Release, Off. of Pub. Affs., U.S. Dep't of Just., 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 (Mar. 8, 2022), https://www.justice.gov/opa/pr/medical-services-contractor-pays-930000-settle-false-claims-act-allegations-relating-medical.
[8] *Id.*
[9] *Id.*
[10] *Id.*
[11] Press Release, Off. of Pub. Affs., U.S. Dep't of Just., Jelly Bean Communications Design and its Manager Settle False Claims Act Liability for Cybersecurity Failures on Florida Medicaid Enrollment Website (Mar. 14, 2023), https://www.justice.gov/opa/pr/jelly-bean-communications-design-and-its-manager-settle-false-claims-act-liability.
[12] *Id.*
[13] *Id.*
[14] *Id.*
[15] *Id.*
[16] *Id.*
[17] Press Release, Off. of Pub. Affs., U.S. Dep't of Just., Consulting Companies to Pay $11.3M for Failing to Comply with Cybersecurity Requirements in Federally Funded Contract (June 17, 2024), https://www.justice.gov/opa/pr/consulting-companies-pay-113m-failing-comply-cybersecurity-requirements-federally-funded; Press Release, Off. of Pub. Affs., U.S. Dep't of Just., Staffing Company to Pay $2.7M for Alleged Failure to Provide Adequate Cybersecurity for COVID-19 Contact Tracing Data (May 1, 2024) [hereinafter Global Insight Press Release], https://www.justice.gov/opa/pr/staffing-company-pay-27m-alleged-failure-provide-adequate-cybersecurity-covid-19-contact.
[18] Global Insight Press Release, https://www.justice.gov/opa/pr/staffing-company-pay-27m-alleged-failure-provide-adequate-cybersecurity-covid-19-contact.
[19] *Id.*
[20] Settlement Agreement Between the United States Department of Justice and Global Insight LLC at ¶ D, https://www.justice.gov/opa/media/1350311/dl?inline (last visited Sept. 20, 2024).
[21] Global Insight Press Release, https://www.justice.gov/opa/pr/staffing-company-pay-27m-alleged-failure-provide-adequate-cybersecurity-covid-19-contact.

[22] *Id.*
[23] Press Release, Off. of Pub. Affs., U.S. Dep't of Just., Consulting Companies to Pay $11.3M for Failing to Comply with Cybersecurity Requirements in Federally Funded Contract (June 17, 2024), https://www.justice.gov/opa/pr/consulting-companies-pay-113m-failing-comply-cybersecurity-requirements-federally-funded.
[24] *Id.*
[25] *Id.*
[26] United States' Complaint-in-Intervention, United States *ex rel.* Craig v. Georgia Tech Rsch. Corp., No. 1:22-cv-02698 (N.D. Ga. Aug. 22, 2024) [hereinafter Georgia Tech Complaint], https://www.justice.gov/opa/media/1364901/dl?inline.
[27] *Id.* ¶¶ 55-61.
[28] *Id.* ¶¶ 14, 18, 62-96.
[29] *Id.* ¶ 12.
[30] *Id.* ¶¶152-154.
[31] *Id.* ¶¶ 155-174.
[32] *Id.* ¶ 174.
[33] *Id.* ¶¶ 175-198.
[34] *Id.* ¶¶ 11, 189.
[35] *Id.* ¶¶ 199-221.
[36] *Id.* ¶ 72.
[37] *Id.* ¶ 200.
[38] *Id.* ¶ 203.
[39] *Id.* ¶ 202.
[40] *Id.* ¶ 205-209.
[41] *Id.* ¶¶ 306-314.
[42] *Id.* ¶¶ 315-328.
[43] *Id.* ¶¶ 329-330.
[44] *Id.* ¶¶ 331-334.
[45] *Id.* ¶¶ 335-336.
[46] Defendant's Motion to Dismiss, United States *ex rel.* Craig v. Georgia Tech Rsch. Corp., No. 1:22-cv-02698, Doc. 34. (N.D. Ga. Oct. 21, 2024).
[47] *Id.* at 11-18, 22-25.
[48] *Id.* at 7.
[49] *Id.* at 25-27.
[50] *Id.* at 36-41.
[51] *Id.* at 36-41.
[52] *Id.* at 38.
[53] *Id.* at 40.
[54] *Id.* at 20 n. 6 (citing United States ex rel. Zafirov v. Fla. Med. Assocs., LLC, 2024 WL 4349242 (M.D. Fla. 2024)).
[55] Defendant's Motion for Judicial Notice and for Court to Consider Documents Under Incorporation by Reference Doctrine, United States *ex rel.* Craig v. Georgia Tech Rsch. Corp., No. 1:22-cv-02698, Doc. 35. (N.D. Ga. Oct. 21, 2024).
[56] Press Release, Off. of Pub. Affs., U.S. Dep't of Just., The Pennsylvania State University Agrees to Pay $1.25M to Resolve False Claims Act Allegations Relating to Non-Compliance with Contractual Cybersecurity Requirements (Oct. 22, 2024), https://www.justice.gov/opa/pr/pennsylvania-state-university-agrees-pay-125m-resolve-false-claims-act-allegations-relating.
[57] Press Release, Off. of Pub. Affs., U.S. Dep't of Just., The Pennsylvania State University Agrees to Pay $1.25M to Resolve False Claims Act Allegations Relating to Non-Compliance with Contractual Cybersecurity Requirements (Oct. 22, 2024), https://www.justice.gov/opa/pr/pennsylvania-state-university-agrees-pay-125m-resolve-false-claims-act-allegations-relating.
[58] Georgia Tech Complaint ¶ 9.
[59] *Id.*
[60] United States *ex rel.* Permenter v. eClinicalWorks, LLC, No. 5:18-cv-382, 2022 WL 17478238, at *1 (M.D. Ga. Dec. 6, 2022).
[61] *Id.* at *3.
[62] *Id.* at *8.
[63] United States *ex rel.* O'Donnell v. Am. at Home Healthcare and Nursing Servs., Ltd., No. 14-cv-1098, 2018 WL 319319, at *1 (N.D. Ill. Jan. 8, 2018); United States *ex rel.* O'Donnell v. Am. at Home Healthcare and Nursing Servs., Ltd., No. 14-cv-1098, Doc. 148 (N.D. Ill. Mar. 14, 2018).
[64] United States *ex rel.* O'Donnell v. Am. at Home Healthcare and Nursing Servs., Ltd., No. 14-cv-1098, 2018 WL 319319, at *7 (N.D. Ill. Jan. 8, 2018).