Westlaw Today

School's back in session: Georgia Tech settles cyber FCA allegations for $875,000

By Tirzah S. Lollar, Esq., Arnold & Porter*

OCTOBER 30, 2025

Just before the end of the fiscal year and the government shutdown, the U.S. Department of Justice (DOJ) announced (https://bit.ly/3X60uHG) Sept. 30 that it had settled (https://bit.ly/3X1E5eF) its cyber FCA allegations against Georgia Tech.

Our readers will recall that the case initially was filed by two former members of Georgia Tech's Cybersecurity Team who alleged (https://bit.ly/4oDZyGj) that the university failed to properly implement the NIST SP 800-171 security controls and that the university had "hundreds of contracts" with the U.S. Department of Defense (DoD).

Unlike the other companies that have settled cyber FCA allegations under DOJ's now four-year-old Civil-Cyber Fraud Initiative, Georgia Tech initially began to litigate the case.

Enter DOJ, which intervened and targeted (https://bit.ly/43J5dmp) its allegations primarily on one particular Georgia Tech lab run by a researcher whose research focuses on cybersecurity.

DOJ apparently had taken numerous depositions during its pre-intervention investigation. Its complaint contains quotes from former employees who said that researchers who brought in significant government contracting money were considered "star quarterbacks" who were allowed to ignore cybersecurity requirements in the university's DoD research contracts "because they found it burdensome" to comply with them and the school's leadership did not want to discourage the researchers from participating in projects that were bringing in substantial federal funding.

DOJ alleged that the lab in question failed to develop a required System Security Plan until three years after the relevant federal research contracts began, and even then, did not include all relevant aspects of the network in the plan. DOJ also alleged that Georgia Tech failed to use antivirus software on the relevant network.

And finally, DOJ alleged that the lab failed to calculate a Supplier Performance Risk System (SPRS) score as required and instead submitted a score in SPRS for a "virtual" campus-wide cybersecurity environment despite internal warnings that doing so could be misleading.

Unlike the other companies that have settled cyber FCA allegations under DOJ's now four-year-old Civil-Cyber Fraud Initiative (https://bit.ly/47OhlzC), Georgia Tech initially began to litigate (https://bit.ly/4qtOzkJ) the case.

It filed a motion to dismiss, arguing that because it performed "fundamental research" under relevant federal contracts, it was not required to comply with the cybersecurity requirements cited in DOJ's complaint and that the government had not adequately pleaded falsity, knowledge, or materiality.

As with many of the cyber FCA settlements to date, there was no allegation that the cyber noncompliances described in the complaint resulted in any breach or exfiltration of data.

DOJ took on each of those arguments in its opposition and notably with respect to materiality, argued, among other things, that "common sense alone supports the materiality of the cybersecurity requirements Defendants allegedly breached," particularly because the DoD had contracted with Georgia Tech to develop technologies that could enable identification of cyber threat actors and limit cyberattacks in the first place and Georgia Tech itself has been victim to such attacks.

We at *Qui Notes* were interested to see how the court would rule, but after briefing was complete, the parties

notified the court that they were in settlement talks and the case ultimately settled without a decision on the motion to dismiss.

The settlement agreement refers to conduct set forth in DOJ's complaint-in-intervention as the Covered Conduct that the parties have agreed to settle. We note that, as with many of the cyber FCA settlements to date, there was no allegation that the cyber noncompliances described in the complaint resulted in any breach or exfiltration of data, though it does state that universities are prime targets for cyberattacks by foreign adversaries and that Georgia Tech has been victim to cyberattacks, including one in 2019 that compromised the records of 1.3 million individuals.

To resolve the case, Georgia Tech agreed to pay $875,000, of which $437,500 is restitution, meaning that Georgia Tech was able to pay only double damages (and no penalties) rather than the treble damages that the statute allows. It is common that a settling defendant would pay less than treble damages in a settlement.

The relators will receive $201,000, just shy of 23% of the settlement amount, as their relator's share for bringing the suit in the first place.

Georgia Tech was able to pay only double damages (and no penalties) rather than the treble damages that the statute allows.

By our count, this is DOJ's fourteenth settlement under the Civil-Cyber Fraud Initiative, and we have yet to see a defendant choose to litigate one of these cases beyond filing a motion to dismiss.

About the author

Tirzah S. Lollar, a partner and co-chair of **Arnold & Porter**'s False Claims Act practice, focuses on white-collar defense and internal and government investigations. She is based in Washington, D.C., and can be reached at tirzah.lollar@arnoldporter.com. This article was originally published Oct. 1, 2025, on the firm's website. Republished with permission.

This article was published on Westlaw Today on October 30, 2025.