Ga. Tech Case Shows DOJ Focus On Higher Ed Cybersecurity

By **Beth Waller and Justin Lugar** (February 7, 2025)

Beth Waller

When the U.S. Department of Justice intervened in a case involving the Georgia Institute of Technology in August, the agency provided a playbook for whistleblowers and prosecutors to bring cases under Title IV of the Higher Education Act.

While Georgia Tech is pushing for dismissal of the False Claims Act case filed against it, which stems from claims from two relators who work or worked as cybersecurity compliance employees for the university, the case demonstrates how many colleges and universities may be unwittingly exposed to a myriad of cybersecurity requirements that, if not followed, could lead to FCA liability.

Justin Lugar

Add in the increased scrutiny from the DOJ's Civil Cyber-Fraud Initiative, or CCFI, which aims to combat cyber threats to the security of sensitive information and critical systems under the FCA, and higher education institutions have a potential ticking time bomb on their hands when it comes to cybersecurity standards.

Further, given that cybersecurity is one of the very few topics with bipartisan support in Washington, the new administration is unlikely to affect the DOJ's enforcement priorities in this space.

Cybersecurity Obligations for Institutions Administering Federal Financial Aid

If there were any doubt, the DOJ has made clear in recent briefings in the Georgia Tech case that the government and its agencies value compliance with regulatory and contractual cybersecurity obligations, particularly when dealing with confidential but unclassified information, or CUI. Presidents Joe Biden, Donald Trump and Barack Obama each issued executive orders addressing the threats posed by malicious cyber actors, and the DOJ's CCFI is an integral part of the National Cybersecurity Strategy Implementation Plan, which was announced by the White House in May.

The DOJ's Playbook in Recent Cases

The DOJ's recent intervention in U.S. v. Georgia Tech Research Corp. and the Georgia

Institute of Technology confirms we should all take the DOJ at its word: Enforcement actions regarding cybersecurity standards in all industries involving federal funds are coming.

In the Georgia Tech case, the DOJ signaled its prioritization of FCA enforcement actions when CUI is in play. Based on its investigation of allegations levied by two whistleblowers — the former associate director of cybersecurity and a former principal information security engineer — the government alleges Georgia Tech submitted false certifications and records beginning in 2019 regarding its purported compliance with the Defense Federal Acquisition Regulation Supplement, or DFARS.

Specifically, the government alleges management at Georgia Tech, including at senior levels, ignored its cybersecurity obligations to accommodate researchers who regularly brought in large sums of government money. Instead of requiring its rainmaking researchers to comply with DFARS, Georgia Tech allegedly ignored its obligations and falsely certified to the U.S. Department of Defense that it complied with the DFARS, knowing that it had never developed (much less implemented) a system security plan, nor required basic security measures as simple as requiring the use of commercial antivirus software on services and researchers' personal computers with access to CUI.

The DFAR regulations at issue in the Georgia Tech case compel DOD contractors to adopt and implement standards established by the National Institutes of Standards and Technology's Special Publication 800-171[1] to obtain, and maintain, research contracts and grants with the DOD. The DOJ's 99-page complaint-in-intervention, and its briefing in opposition to Georgia Tech's motion to dismiss filed in late December, demonstrate the importance of compliance with regulations aimed at securing CUI, such as that presented under Title IV. Moreover, the DOJ makes clear that compliance with regulations securing CUI is material under the FCA.

So, while the underlying regulatory scheme may vary depending on the federal agency, the DOJ's first CCFI intervention confirms that the government can and will venture into other areas where CUI is at risk.

For colleges and universities, federal financial aid is a particularly appealing target given the sheer volume of at-risk transactions and the $114.9 billion of federal funds administered by higher education institutions in 2023-2024.

Cybersecurity Standards Required of Title IV Institutions Administering Financial Aid

Like the regulatory regime that the DOD implemented to protect CUI in its contracts, the U.S. Department of Education also mandated certain minimum cybersecurity standards to participate in federal financial aid.

Over the years, the Education Department has proactively reminded higher education institutions of their obligations under the Student Aid Internet Gateway enrollment agreement and the federal student aid program participation agreement, or PPA. In a slow but steady buildup commencing in earnest in 2015 — not unlike the path forged by the DOD in the Georgia Tech case — the Education Department has methodically set forth its expectations of higher education institutions regarding cybersecurity standards.

Furthermore, the Education Department has previously highlighted its reliance on the PPA signed by every participating higher education institution, which demands compliance with the Gramm-Leach-Bliley Act. The GLBA, in turn, treats higher education institutions as "financial services organizations" and imposes additional substantive cybersecurity requirements "to ensure the security and confidentiality of student financial aid records and information," according to a 2016 Dear Colleague Letter from the then-undersecretary of the Education Department.[2]

Combined with guidance from the Education Department and the Federal Trade Commission regarding safeguarding consumer information under the GLBA, the burden on higher education institutions is high when it comes to protecting students' personal information.

As a result, colleges and universities must establish written incident response plans. Plus, according to Title 15 of the Code of Federal Regulations, Section 314.4(i), "regularly and at least annually," the qualified individual responsible for the security program must "report in writing" to the board, directors or equivalent governing body on the "overall status of the information security program and your compliance with this part," as well as any material matters involving risk assessment and management, security threats or events, violations (if any) and responses.[3]

Last January, the Education Department also issued its Information Technology System and Information Integrity Standard as a result of its obligations under the Federal Information Security Modernization Act, or FISMA, and Office of Management and Budget Circular A-130, which mandates a minimum standard for securing sensitive

information.[4]

As a result, institutions of higher education participating in federal student aid programs have mandatory obligations under several statutory and regulatory schemes, including (1) the GLBA, (2) the FTC's final rules regarding safeguarding customer/student information, (3) FISMA, and (4) other published Education Department standards.

As noted above, every Title IV financial aid participant must sign a PPA requiring specific compliance with the FTC regulations, the GLBA, FISMA and OMB Circular A-130, meaning every institution has made affirmative representations and certifications of compliance.

Protecting CUI is Material, and All Institutions Are Subject to FCA Liability

Like DOD contractors bound by the DFARS, higher education institutions must meet certain minimum requirements regarding cybersecurity and the protection of confidential unclassified information as a condition for doing business with the federal government. That means each of the nearly 6,000 colleges and universities that administer roughly $110 billion of federal financial aid annually must meet the minimum security standards discussed above.

The DOJ has made clear that protecting students' financial and other sensitive information is a material condition of participation, and payment, in federal student aid programs. Enforcement of these material conditions of participation in federal programs is a core purpose of the FCA. The DOJ's CCFI will undoubtedly look hard at any allegations of false or fraudulent certifications or representations about an institution's cybersecurity program.

DOJ Has Targeted Higher Ed Before

It also bears mentioning that the DOJ has not shied away from penalizing higher education institutions in the past, albeit in the context of preventing and deterring incentive-based compensation for student recruitment. These prior enforcement actions under the FCA demonstrate that the DOJ will aggressively pursue compliance failures and will not hesitate to demand hefty financial penalties, as reflected in the following:

- The $67.5 million University of Phoenix settlement in 2009;[5]
- The $95.5 million Education Management Corp. settlement in 2015;[6]
- The $13 million Education Affiliates settlement in 2015;[7] and

- The $2.5 million North Greenville University settlement in 2019.[8]

There can be little doubt then that the DOJ will ramp up enforcement to protect CUI and students' sensitive financial information, just as the DOJ used the FCA to eradicate incentive-based compensation to protect students from predatory recruitment behavior.

Given the history of the DOJ's use of the FCA vis-à-vis the Higher Education Act and the goals of the DOJ's CCFI, higher education institutions should heed Claus Moser's adage: "Education costs money, but then so does ignorance," and recognize that ignorance or apathy are more costly than proactive measures to exceed the minimum requirements for protecting and securing CUI.[9]

They should also take note of the warnings in the DOJ's Georgia Tech complaint (and subsequent briefing), and immediately invest in robust cybersecurity measures so that they may focus on educating future generations, not paying for the mistakes of the past.

Beth Burgin Waller is a principal, and chair of the cybersecurity and data privacy practice, at Woods Rogers Vandeventer Black PLC.

Justin Lugar is of counsel at the firm. He was a former assistant U.S. attorney in the Western District of Virginia.

[1] NIST stands for the National Institutes of Standards and Technology, a sub-agency housed within the U.S. Department of Commerce.

[2] (GEN-16-12) Subject: Protecting Student Information, https://fsapartners.ed.gov/knowledge-center/library/dear-colleague-letters/2016-07-01/gen-16-12-subject-protecting-student-information.

[3] 15 C.F.R. § 314.4(i).

[4] U.S. Department of Education, Information Technology (IT) System and Information Integrity (SI) Standard, Jan. 19, 2024, available at https://www.ed.gov/sites/ed/files/fund/contract/about/acs/2024-si-system-information-and-integrity-standard.pdf (last visited Oct. 24, 2024); Revision of OMB Circular No. A-130, "Managing Information as a Strategic Resource", 81 Fed. Reg. 49689 (July 28, 2016).

[5] https://www.justice.gov/opa/pr/university-phoenix-settles-false-claims-act-lawsuit-675-million.

[6] https://www.justice.gov/opa/pr/profit-college-company-pay-955-million-settle-claims-illegal-recruiting-consumer-fraud-and.

[7] https://www.justice.gov/opa/pr/profit-education-company-pay-13-million-resolve-several-cases-alleging-submission-false.

[8] https://www.justice.gov/opa/pr/south-carolina-university-pay-25-million-settle-false-claims-act-allegations-arising.

[9] Baron Claus Moser, Our Need for an Informed Society: Presidential Address to the British Association for the Advancement of Science, Brangwyn Hall, Swansea, UK, Aug. 20, 1990).