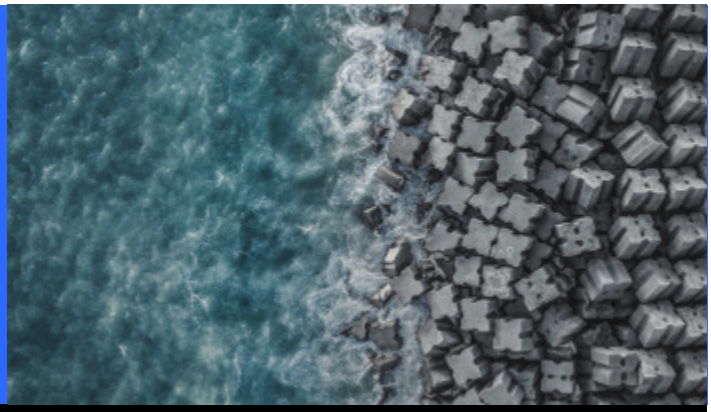
GIBSON DUNN



False Claims Act Update August 12, 2025

DOJ Ends July 2025 with Two Groundbreaking FCA Settlements in the Cybersecurity Space

The settlements reinforce the DOJ's FCA cybersecurity efforts and also preview an expansion into enforcing cybersecurity in the healthcare space and against private equity firms and their portfolio companies.

On July 31, 2025, the Department of Justice broke new ground in its False Claims Act (FCA) cybersecurity enforcement efforts by resolving an FCA matter based on the Federal Drug Administration's new cybersecurity requirement and by announcing a settlement against a private equity firm and one of its portfolio companies. Both settlements reinforce what the industry has already known since the announcement of the DOJ's Civil Cyber Fraud Initiative: the DOJ remains steadfast in policing cybersecurity enforcement though the FCA.

The Illumina Inc. Settlement

The DOJ's settlement with Illumina not only represents one of the larger FCA cybersecurity settlements historically (coming in at $9.8 million),[1] but also opens the door to FCA enforcement of the FDA's new cybersecurity requirements. The settlement resolves a 2023 *qui tam* action brought by a former Illumina employee involved in the cybersecurity of its genomic-sequencing products.[2] The relator alleged that Illumina defrauded the federal government when selling genomic-sequencing software with extensive cybersecurity vulnerabilities to federal agencies and government funded health programs. Notably, the products allegedly provided "elevated privileges to everyday users by defaults," which the relator described as "analogous to having super admin rights of a database."[3] Consequently, thousands of the company's everyday users

were allegedly able to access and manipulate customers' HIPAA-protected data without detection, "change product configurations and settings[,] install unauthorized applications[,] grant third-parties access to the system[, and] disable firewalls and other operating-system level protections."[4]

The FCA theory hinged on 2024 FDA cybersecurity regulations. Specifically, the FDA regulates medical devices' product safety under the Quality Systems Regulation, 21 C.F.R. § 820, which requires companies to implement a comprehensive cybersecurity risk management program.[5] The settlement resolves the first-known FCA enforcement action stemming from the FDA's new cybersecurity regulations, indicating the DOJ's steady focus on expanding its cybersecurity enforcement into the healthcare space.

Aero Turbine/Gallant Settlement

In another first, the DOJ settled an FCA cybersecurity action against a private equity firm, along with one of its portfolio companies. On July 31, 2025, the DOJ announced that it settled an FCA matter with private equity firm Gallant Capital Partners, LLC and its portfolio company, defense contractor Aero Turbine, Inc.[6] According to the settlement agreement, Aero Turbine allegedly failed to comply with NIST SP 800-171 as required by the DFARS clause 252.204-7012 in connection with its contracts with the Air Force and, under direction from a Gallant employee, improperly provided access to Air Force controlled unclassified information (CUI) to a software company based in Egypt.[7] The settlement agreement acknowledges Aero Turbine's and Gallant Capital's self-disclosure and cooperation, for which they received credit.

This is the first cybersecurity settlement with a private equity firm, and the first FCA settlement involving a private equity firm since at least 2021.

The Future for FCA Cybersecurity Actions

These two settlements not only reinforce the DOJ's FCA cybersecurity efforts, but they also preview an expansion into enforcing cybersecurity in the healthcare space and against private equity firms and their portfolio companies.

[1] *See* Press Release, U.S. Dep't of Justice Office of Public Affairs, Illumina Inc. to Pay $9.8M to Resolve False Claims Act Allegations Arising from Cybersecurity Vulnerabilities in Genomic Sequencing Systems (July 31, 2025), https://www.justice.gov/opa/pr/illumina-inc-pay-98m-resolve-false-claims-act-allegations-arising-cybersecurity.

[2] Complaint, *United States ex rel. Lenore v. Illumina, Inc.*, 23-cv-00372-MSM (D.R.I. Sept. 8, 2023), Dkt. No. 1.

[3] *Id.* ¶ 7.

[4] *Id.* ¶ 55.

[5] 21 C.F.R. § 820.

[6] *See* Press Release, U.S. Dep't of Justice Office of Public Affairs, California Defense Contractor and Private Equity Firm Agree to Pay $1.75M to Resolve False Claims Act Liability Relating to Voluntary Self-Disclosure of Cybersecurity Violations (July 31, 2025), https://www.justice.gov/opa/pr/california-defense-contractor-and-private-equity-firm-agree-pay-175m-resolve-false-claims.

[7] *Id.*; *see also* Settlement Agreement between the Dep't of Justice; Aero Turbine, Inc.; and Gallant Capital, LLC, (July 31, 2025), available at https://www.justice.gov/opa/media/1409651/dl.

The following Gibson Dunn lawyers prepared this update: Winston Y. Chan, Jake M. Shields, and Samantha O. Hay.

Gibson Dunn lawyers regularly counsel clients on the False Claims Act issues and are available to assist in addressing any questions you may have regarding these issues. Please 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 practice group:

False Claims Act/Qui Tam Defense:

Washington, D.C.
Jonathan M. Phillips – Co-Chair (+1 202.887.3546, jphillips@gibsondunn.com)
Stuart F. Delery (+1 202.955.8515,sdelery@gibsondunn.com)
F. Joseph Warin (+1 202.887.3609, fwarin@gibsondunn.com)
Jake M. Shields (+1 202.955.8201, jmshields@gibsondunn.com)
Gustav W. Eyler (+1 202.955.8610, geyler@gibsondunn.com)
Lindsay M. Paulin (+1 202.887.3701, lpaulin@gibsondunn.com)
Geoffrey M. Sigler (+1 202.887.3752, gsigler@gibsondunn.com)
Joseph D. West (+1 202.955.8658, jwest@gibsondunn.com)

San Francisco
Winston Y. Chan – Co-Chair (+1 415.393.8362, wchan@gibsondunn.com)

New York
Reed Brodsky (+1 212.351.5334, rbrodsky@gibsondunn.com)
Mylan Denerstein (+1 212.351.3850, mdenerstein@gibsondunn.com)

Denver
John D.W. Partridge (+1 303.298.5931, jpartridge@gibsondunn.com)
Ryan T. Bergsieker (+1 303.298.5774, rbergsieker@gibsondunn.com)
Monica K. Loseman (+1 303.298.5784, mloseman@gibsondunn.com)

Dallas
Andrew LeGrand (+1 214.698.3405, alegrand@gibsondunn.com)

Los Angeles
James L. Zelenay Jr. (+1 213.229.7449, jzelenay@gibsondunn.com)
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)
Dhananjay S. Manthripragada (+1 213.229.7366, dmanthripragada@gibsondunn.com)