DOJ Settlement With Medical Technology Company Signals Expanding Cybersecurity FCA Risk for Life Sciences Companies

Skadden

August 7, 2025

If you have any questions regarding the matters discussed in this memorandum, please contact the attorneys listed on the last page or call your regular Skadden contact.

One Manhattan West
New York, NY 10001
212.735.3000

Executive Summary

- **What is new:** DOJ announced a $9.8 million FCA settlement with Illumina Inc. to resolve claims arising out of alleged cybersecurity deficiencies in DNA sequencing systems Illumina sold to government agencies.
- **Why it matters:** The case underscores that in addition to traditional FDA enforcement risk, cybersecurity failures may expose medical device manufacturers to increasing FCA risk.
- **What to do next:** Companies should proactively assess and address cybersecurity vulnerabilities, ensure the accuracy of their cybersecurity compliance representations, and stay abreast of evolving regulatory expectations to mitigate potential liability.

On July 31, 2025, the Department of Justice (DOJ) announced a $9.8 million settlement with Illumina Inc., a leading manufacturer of DNA sequencing systems, to resolve potential False Claims Act (FCA) liability related to alleged cybersecurity shortcomings in products sold to government agencies.

This appears to mark the first FCA resolution with a medical device manufacturer based on cybersecurity deficiencies, underscoring DOJ's growing focus on cybersecurity compliance in the life sciences sector. The case highlights that medical technology companies face increasing FCA risk not only from traditional regulatory enforcement, but also from alleged failures to meet cybersecurity standards — particularly when those failures result in false representations to the government.

As the Illumina settlement demonstrates, companies should consider:

- Proactively assessing and addressing cybersecurity vulnerabilities.
- Ensuring the accuracy of their compliance representations.
- Staying abreast of evolving regulatory expectations to mitigate potential liability.

Summary of Allegations

In September 2023, the relator — a former Illumina platform management director — filed a *qui tam* complaint alleging that Illumina violated the FCA by submitting and causing others to submit claims for payment by federal payors while knowingly concealing or misrepresenting the purportedly deficient cybersecurity condition of its genomic sequencing products.

The relator alleged that Illumina submitted direct claims to federal agencies to which it sold its sequencing systems, and that Illumina's genomic testing provider customers submitted claims to federal health care programs for testing that utilized Illumina's systems.

The complaint further alleged three cybersecurity failings by Illumina:

1. Granting everyday users of its systems elevated privileges that allowed them to access and manipulate confidential patient health data.
2. Hard-coding login credentials directly into its software code.
3. Failing to adequately protect its devices from insider threats.

DOJ Settlement With Medical Technology Company Signals Expanding Cybersecurity FCA Risk for Life Sciences Companies

The relator asserted that these alleged failures violated numerous requirements of the Food and Drug Administration's (FDA's) Quality System Regulation (QSR), 21 C.F.R. Part 820, including:

- Part 820.30's design control requirements, which "include software validation and risk analysis."
- Part 820.100's corrective and preventive action (CAPA) requirements, which the relator asserted required Illumina to "identify and investigate product and quality problems" and "take appropriate and effective corrective and/or preventative action" to address cybersecurity vulnerabilities in its genomic sequencing systems, both pre- and post-launch.
- Part 820.20's requirements for "management with executive responsibility," whom the relator alleged were made aware of the purported cybersecurity deficiencies but "actively discounted, disregarded, and suppressed attempts" by employees to raise issues regarding vulnerabilities.

In addition, the relator generally alleged that Illumina made "materially false certifications to the Government about the cybersecurity protections of its products," including by not fully disclosing purported cybersecurity vulnerabilities, violating requirements under servicing contracts for systems sold to the government, and failing to comply with program rules for privacy and data security included in government grant programs.

Key Aspects of the Illumina Resolution

The Illumina resolution further reinforces that cybersecurity remains a significant enforcement priority for DOJ, which has been building a record of enforcing cybersecurity compliance through the FCA. Since announcing its Civil Cyber-Fraud Initiative in October 2021, DOJ has pursued several civil FCA cases based on alleged cybersecurity deficiencies and, in September 2024, announced its first intervention in a *qui tam* suit brought by a private relator.[1]

DOJ has since settled a number of other cybersecurity-based FCA cases and, indeed, announced another such resolution (with defense contractor Aero Turbine Inc. and private equity company Gallant Capital Partners LLC) on the same day as the Illumina settlement announcement.

While cybersecurity-based FCA cases are becoming quite common, Illumina appears to be the first such case involving a medical device manufacturer.

Following the announcement of DOJ's Civil Cyber-Fraud Initiative, we explored potential theories of liability by which alleged medical device cybersecurity failures might give rise to FCA liability.[2] These included so-called "fraud on the FDA," which asserts that a manufacturer obtained approval or clearance to market and sell a medical product based on materially false statements or omissions, as well as sales of materially defective products.

The Illumina resolution does not rely on these theories but does appear to implicitly embrace the alleged QSR violations articulated in the relator's complaint. DOJ's settlement agreement asserts that Illumina's claims for systems it sold to various government agencies "were false, regardless of whether any actual cybersecurity breaches occurred, because [Illumina's systems] had cybersecurity vulnerabilities, and Illumina did not have an adequate product security program and sufficient quality systems to identify and address [these] vulnerabilities."

More specifically, DOJ asserts that Illumina's claims "were false because Illumina:

- knowingly failed to incorporate product cybersecurity in its software design, development, installation, and on-market monitoring;
- failed to properly support and resource personnel, systems, and processes tasked with product security;
- failed to adequately correct design features that introduced cybersecurity vulnerabilities in [Illumina's systems]; and
- falsely represented that [the systems] adhered to cybersecurity standards, including [those] of the International Organization for Standardization and National Institute of Standards and Technology."

[1] *See* our client alerts "DOJ Enters First Intervention in Cybersecurity *Qui Tam*" (September 6, 2024), "Contractors Settle Cyber Fraud Claims Alleging Ignored Security Measures" (July 2, 2024) and "Cyber Fraud Alleged by Former CIO for Purported Noncompliance With DoD Cyber Requirements" (October 30, 2023).

[2] *See* our November 2023 article "Increased Focus on Cybersecurity Could Pose False Claims Act Exposure Risk for Life Sciences Companies."

DOJ Settlement With Medical Technology Company Signals Expanding Cybersecurity FCA Risk for Life Sciences Companies

Notably, DOJ does not cite the QSR — or even FDA requirements generally — as the basis for the alleged falsity of Illumina's claims. Nevertheless, the clear implication of the resolution is that QSR failures may lead to FCA liability where they result in cybersecurity deficiencies that, in turn, render false representations to the government regarding cybersecurity compliance.

Considerations for Medical Technology Companies

In addition to confirming the government's continuing focus on cybersecurity compliance, the Illumina resolution highlights the increased risk that medical device manufacturers may face in that regard.

As we have previously discussed, the Food and Drug Omnibus Reform Act (FDORA) created the concept of a "cyber device," which is one that:

- Includes software.
- Is able to connect to the internet.
- Could be vulnerable to cybersecurity threats.

Cyber devices are subject to specific regulation and enforcement mechanisms under the Food, Drug and Cosmetic Act; failure to adhere to those requirements, as well as preexisting QSR requirements, may lead to traditional FDA enforcement, including warning letters and recalls.

Separate and apart from these threats, as the Illumina resolution shows, medical device manufacturers that sell products relied on directly or indirectly by government agencies may face FCA exposure insofar as they make representations or agree to contractual obligations involving cybersecurity compliance.

To mitigate against potential exposure, medical device companies should consider:

- Reviewing existing and future product offerings for all cybersecurity vulnerabilities, including in the company's quality system procedures, IT infrastructure and software development processes, especially where sensitive health information is concerned.
- Addressing any potential or actual cybersecurity deficiencies in accordance with FDA and other cybersecurity regulations and industry best practices, including processes for receiving, evaluating and addressing reports from external security researchers.
- Confirming that the software development life cycle includes secure coding standards, formal threat modeling, risk-based testing and patch deployment protocols.
- Ensuring the accuracy of all representations to FDA and potential customers concerning the cybersecurity of their products. Document gaps and corrective actions where necessary.
- Tracking regulatory developments regarding cybersecurity and ensuring continuing compliance, as this area remains a government priority.

Contacts

Avia M. Dunn
Partner / Washington, D.C.
202.371.7174
avia.dunn@skadden.com

Bradley A. Klein
Partner / Washington, D.C.
202.371.7320
bradley.klein@skadden.com

David A. Simon
Partner / Washington, D.C.
202.371.7120
david.simon@skadden.com

Maya P. Florence
Partner / Boston
617.573.4805
maya.florence@skadden.com

William E. Ridgway
Partner / Chicago
312.407.0449
william.ridgway@skadden.com

Rachael K. Cox
Associate / Houston
713.655.5153
rachael.cox@skadden.com