# Hardening Software Security: DOJ's Civil Cyber Fraud Settlements Continue to Illumina[te] the Importance of Cybersecurity

**Client Alert** | 3 min read | 08.26.25

On July 31, 2025, the Department of Justice (DOJ) **announced** that Illumina, Inc. will pay $9.8 million to resolve allegations that it violated the False Claims Act (FCA) by selling genomic sequencing systems with software containing cybersecurity vulnerabilities to federal agencies. This is the first FCA **settlement** involving claims that a medical manufacturer failed to incorporate adequate product cybersecurity into its software design and development.

The allegations were first made in *United States ex rel. Lenore v. Illumina Inc.*, No. 1:23-cv-00372 (D.R.I.), a *qui tam* action filed by Illumina's former Director for Platform Management, On-Market Portfolio in September 2023. The relator alleged that, between February 2016 and September 2023, Illumina knowingly sold genomic sequencing systems to government agencies without adequate security programs or quality systems to identify and address software vulnerabilities. The complaint further alleged that Illumina failed to properly resource personnel and processes responsible for product security, did not remediate design features introducing cybersecurity risks, and misrepresented the software's adherence to required cybersecurity standards.

According to the government, Illumina's actions included:

- Failing to incorporate product cybersecurity into the lifecycle of its genomic sequencing systems, including design, development, and post-market monitoring;
- Inadequately supporting and resourcing the personnel, systems, and processes responsible for product security;
- Not correcting design features that introduced known cybersecurity vulnerabilities; and
- Falsely certifying compliance with cybersecurity standards published by the International Organization for Standardization (ISO) and the National Institute of Standards & Technology (NIST) in representations to federal agencies.

As a result of these actions, the government contended that Illumina submitted false claims to numerous agencies for its genomic sequencing systems. Notably, the government asserted that the claims were false regardless of whether any actual cybersecurity breaches occurred. As part of the settlement, Illumina agreed to pay $9.8 million, with $1.9 million of that awarded to the whistleblower as a relator's share. In its press release, the government emphasized that the settlement underscores the importance of cybersecurity in the handling of sensitive genetic information and reinforces DOJ's commitment to hold federal contractors accountable for cybersecurity risks.

## Key Takeaways

- DOJ is not focused solely on the security of contractor systems. DOJ is continuing to explore the full scope of cybersecurity shortcomings, probing down to the software and hardware level of products provided to the government, particularly in the life sciences, medical technology, and digital health space. This represents the first FCA settlement grounded in software vulnerabilities since DOJ's **early salvos** in 2019.
- Federal contractors must ensure that secure software development is embedded throughout the product lifecycle, from design to post-market monitoring. Overlooking it in the federal marketplace carries risks of not only operational downsides but also regulatory enforcement.
- NIST is not the only cybersecurity standard that matters. False representations of compliance with any cybersecurity standard for products or software, including ISO standards less frequently seen in government contracts, can lead to allegations of FCA liability.
- Whistleblowers remain key drivers of FCA enforcement in the cybersecurity space. With substantial financial incentives available under the statute's *qui tam* provisions, federal contractors should anticipate more whistleblower activity, especially among personnel expressing concerns about cybersecurity compliance.

## Contacts

**Nkechi Kanu**
Partner
Washington, D.C. D | +1 202.624.2872
nkanu@crowell.com

**Kate M. Growley**
Partner, Crowell Global Advisors Senior Director
Washington, D.C. D | +1.202.624.2698
Washington, D.C. (CGA) D | +1 202.624.2500
kgrowley@crowell.com

**Brian Tully McLaughlin**
Partner
Washington, D.C. D | +1.202.624.2628
bmclaughlin@crowell.com

**Michael G. Gruden**
Partner
Washington, D.C. D | +1.202.624.2545
mgruden@crowell.com

 

**Jessica R. Chao**
Associate
She/Her/Hers

Denver D | +1.303.524.8637
jchao@crowell.com

**Jasmine L. Masri**
Associate
She/Her/Hers

Washington, D.C. D | +1.202.624.2715
jmasri@crowell.com

 