LEECH | TISHMAN

Navigating DOJ Cybersecurity Enforcement: FCA Risks and Updated Regulatory Compliance

By: Lydia A. Pappas, Esq.

Published March 5, 2026

Over the past several years, the Department of Justice ("DOJ") has vigorously pursued enforcement actions related to Cybersecurity Fraud under a variety of new and developing regulations. Now, with the Cybersecurity Maturity Model Certification ("CMMC") rule finally enacted, awareness and compliance are crucial for companies that aim to avoid costly penalties.

Billions in federal funds are tied to sensitive defense, health, and research projects, making compliance with cybersecurity requirements a high-stake obligation for any company contracting with either a state or the Federal Government. Additionally, since 2021, the DOJ's Civil Cyber-Fraud Enforcement efforts have resulted in almost $77 million in settlements, having impacted nearly every industry.

The False Claims Act ("FCA") and its qui tam provisions have been the DOJ's most effective tool in its enforcement efforts. Qui tam statutes enlist the public, largely company insiders, to initiate civil suits on the Government's behalf seeking per-claim civil penalties and forfeitures from companies and individuals who have defrauded the Government. This is not limited to the submission of false claims but includes avoidance or non-compliance with applicable regulatory or contractual provisions. This is known as a false certification theory under the FCA, and these have been rising in prominence in recent enforcement actions. The FCA also rewards the whistleblowers, called Relators, with a portion of the recovered proceeds.

This all means that if a company fails to comply with its contractual and regulatory obligations in safeguarding its data, it could cost them millions. Accurate reporting, documented controls, proactive monitoring and remediation, and overall transparency are essential to maintaining trust with agency partners and avoiding FCA exposure at a time where the Government is laser focused on cybersecurity compliance. Indeed, the Government's overall FCA enforcement efforts have soared in the past few years, leading to a record $6.8 billion in recoveries in 2025. While healthcare remains the majority of recoveries, DOJ officials have explicitly stated that key areas of enforcement headed into 2026 are cybersecurity, customs and tariffs, and government contracting. Thus, scrutiny in these areas will be fierce moving forward.

Leech Tishman's Labor & Employment attorneys regularly counsel clients on compliance with statutory and common law requirements. Our team is prepared to assist your company in understanding and implementing the obligations and compliance measures required under the DOJ's Cybersecurity Fraud Enforcement program. For assistance or additional information, please contact Lydia A. Pappas at lpappas@leechtishman.com, attorney in Leech Tishman's Labor & Employment Practice Group.