Articles + Publications | December 9, 2025

FCA Settlement Signals Increased Cybersecurity Focus

WRITTEN BY

Michael A. Schwartz | Allison O'Neil | Jaycee E. Parker | Jessica McClellan

The U.S. Department of Justice (DOJ) recently announced a $421,234 settlement with Swiss Automation Inc. to resolve alleged False Claims Act (FCA) violations related to its failure to provide adequate cybersecurity for technical drawings of parts supplied to Department of Defense (DoD) contractors. This settlement resolves a qui tam action filed under the whistleblower provisions of the FCA in the Northern District of Illinois. (*United States ex rel. Gomez v. Swiss Automation Inc.*, No. 1:22-cv-4328 (N.D. Ill.))

Swiss Automation Inc. is an Illinois-based machining business that supplies alloy and metal parts to commercial and government customers in various industries. The company allegedly failed to provide adequate security by implementing cybersecurity controls specified in the Defense Federal Acquisition Regulation Supplement (DFARS) 252.204-7012, causing the submission of false claims for payment. These cybersecurity controls are intended to protect certain DoD information and have applied to DoD contracts, subcontracts, and similar contractual instruments since 2017. Such control obligations will continue under the recently finalized Cybersecurity Maturity Model Certification (CMMC) program, which assesses defense contractor compliance with existing information safeguarding requirements for federal contract information and controlled unclassified information.

The settlement agreement is neither an admission of liability by Swiss Automation, nor a concession that the United States' claims are not well founded. This recent action underscores the DOJ's heightened focus on violations of federal cybersecurity laws and regulations in light of increased cybersecurity threats, particularly those targeting government contractors. As these threats evolve, "suppliers to defense contractors must be vigilant and take the steps required to protect sensitive government information from bad actors," according to DOJ Assistant Attorney General Brett A. Shumate.

Key Takeaways:

- DOJ is investing significant resources into holding government contractors, subcontractors, and suppliers accountable for their cybersecurity obligations to DoD.
- The DFARS control requirements have applied since 2017 and will continue under the finalized CMMC program, which will assess and verify contractor compliance for protecting federal contract information and controlled unclassified information.
- Inadequate cybersecurity controls can trigger FCA exposure.

Companies operating in the relevant sectors should anticipate increased scrutiny and enforcement actions related to cybersecurity regulation. Businesses with government contracts are encouraged to review their compliance programs and ensure that robust measures are in place to safeguard federal contract information, assess potential

risks, and comply with all applicable controls and federal regulations to prevent cybersecurity violations.

Troutman Pepper Locke is monitoring the DOJ's evolving trends and priorities closely. If you have questions about how these priorities may impact your business or wish to begin evaluating your existing compliance procedures, please contact a member of our White Collar Litigation + Investigations team or our Privacy + Cyber group.

RELATED INDUSTRIES + PRACTICES

- White Collar Litigation + Investigations