wiley

ALERT

DOJ Continues Crackdown on Cybersecurity Compliance with $1.25M FCA Settlement

October 28, 2024

The Department of Justice (DOJ) secured another win for its Civil Cyber-Fraud Initiative last week when it resolved a False Claims Act (FCA) action[1] alleging Pennsylvania State University (Penn State) failed to comply with cybersecurity requirements for more than a dozen Department of Defense (DoD) and National Aeronautics and Space Administration (NASA) contracts and subcontracts. The $1.25M resolution with the university comes two years after a chief information officer for Penn State's Applied Research Laboratory brought the case under the FCA's *qui tam* provisions. It also follows a prolonged stay the parties requested specifically to permit DOJ sufficient time to complete its investigation into the alleged conduct.

This is the second settlement this month under the Civil Cyber-Fraud Initiative, and its fifth major action of 2024—by far the busiest year for the three-year-old Initiative. The Civil Cyber-Fraud Initiative leverages the FCA to hold accountable contractors and federal grant recipients that put U.S. information or systems at risk by knowingly providing deficient cybersecurity products or services, knowingly misrepresenting their cybersecurity practices or protocols, or knowingly violating obligations to monitor and report cybersecurity incidents and breaches. Just last week, ASRC Federal Data Solutions LLC agreed to pay more than $300k and waive more than $875k in potentially reimbursable remediation costs to resolve allegations that it failed to properly secure Medicare beneficiary data. Here, unlike in the ASRC case, there were no allegations that a third party ever breached any secured data within Penn State's custody; Penn State's alleged noncompliance in and of itself was enough to attract DOJ attention.

Authors

Brandon J. Moss
Partner
202.719.7554
bmoss@wiley.law

Elizabeth K. Drill
Associate
202.719.3113
edrill@wiley.law

Practice Areas

Civil Fraud, False Claims, *Qui Tam* and Whistleblower Actions

White Collar Defense & Government Investigations

The Penn State Settlement and the Underlying FCA Lawsuit

The covered conduct resolved in the settlement includes allegations that, from January 2018 to November 2023, Penn State failed to implement certain cybersecurity controls required by its government contracts or develop and implement plans of action designed to correct deficiencies and reduce vulnerabilities in informational technology (IT) systems involved in contract performance. Specifically, the settlement alleges that Penn State did not implement certain National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 security requirements for its handling of unclassified information, in violation of NASA Federal Acquisition Regulation Supplement (FARS) 1852.204-76 and Defense Federal Acquisition Regulation Supplement (DFARS) clauses 252.204-7008 and 252.204-7012. Furthermore, DFARS clauses 252.204-7019 and 252.204-7020 require DoD contractors—like Penn State—to submit summary level scores reflecting the status of their compliance with applicable cybersecurity requirements to the DoD's Supplier Performance Risk System (SPRS). Penn State purportedly submitted cybersecurity assessment scores that showed that the university had not implemented certain controls, misrepresented the dates by which it expected to implement the necessary cybersecurity protocols, and never pursued a plan of action to satisfy compliance requirements. DOJ additionally alleged that Penn State did not use an external cloud service provider that met Federal Risk and Authorization Management Program (FedRAMP) security requirements, as mandated by DFARS 252.204-7012.

Notably, the covered conduct in DOJ's settlement with Penn State went beyond the allegations that appear in the Relator's First Amended Complaint (FAC) in the underlying FCA action. Although the basic facts in the settlement are true to the FAC (*i.e.*, that Penn State did not follow certain NIST SP 800-171 security protocols and failed to use a sufficiently secure external cloud service provider), there are marked differences between the allegations articulated in the settlement and those detailed in the FAC. For example, while the settlement cites knowing violation of NASA FARS 1852.204-76 as a basis for liability, the Relator never specifically alleged that Penn State flouted that regulation. Additionally, the settlement's recitation of what was wrong with the summary level scores varied considerably from the Relator's theory of wrongdoing regarding the SPRS submissions—that Penn State filed templates in lieu of required risk assessments. A certain level of differentiation is to be expected given that the precise articulation of covered conduct set forth in an FCA settlement agreement is almost always the product of significant negotiation. However, here, the addition of specific regulations not mentioned in the FAC appears to be a product of the DOJ's extended investigation and evidence that DOJ is, indeed, committing substantial resources not only to validate relator allegations, but find additional violations.

Also of note, this case illustrates a growing trend of sophisticated relators bringing forward cybersecurity noncompliance allegations. Even though the Relator may have lacked information about specific contracts, not knowing the details of purportedly fraudulent claims, and missed the alleged violation of a specific NASA regulation, he was sufficiently knowledgeable about the DFARS and NIST requirements to raise credible concerns over what he viewed as noncompliance with data security protocols. Moreover, the Relator was also able to allege in detail multiple instances in which he purportedly raised compliance concerns and cybersecurity deficiencies that the university either ignored or concealed.

Takeaways

The Penn State settlement serves as the most recent warning to government contractors of DOJ's increased scrutiny on cybersecurity compliance. As is evident here, whistleblower complaints can and do instigate thorough, independent government investigations. What's more, the government does not need a data breach to pursue government contractors accused of knowing noncompliance with cybersecurity requirements—this is at least the second *qui tam* settlement this year not involving an actual, identifiable breach.

This case also highlights the critical role that IT employees can play in surfacing allegations of misconduct in the cybersecurity space—an area with complex and technical regulations and in which assessing noncompliance often requires a high level of expertise and inside knowledge. Furthermore, the parties' settlement does not provide a forfeiture amount or another specific basis for the $1.25M figure, leaving open the question of how DOJ is inclined to calculate damages when a government contractor misstates its cybersecurity compliance and there is no breach or evidence of specific loss. Ultimately, with DOJ seemingly more ready than ever to act on credible reports of known cybersecurity violations, companies must develop strong internal controls designed to facilitate compliance, quickly detect and remediate issues, and ensure that reports of noncompliance are taken seriously.

Wiley's White Collar Defense & Government Investigations practice has extensive experience with the False Claims Act (FCA), particularly defending against government and *qui tam* whistleblower actions under the FCA. Should you have any questions, please contact one of the listed attorneys.

[1] *See U.S. ex rel. Decker v. Pennsylvania State Univ.*, No. 2:22-cv-03895 (E.D. Pa.).