Alert

February 26, 2024

COZEN O'CONNOR

Are You Secure? DOJ's Cyber-Fraud Initiative and Heightened FCA Enforcement

False Claims Act (FCA) enforcement has routinely targeted false information supplied to Medicare and Medicaid. A new trend in false-reporting cases is emerging under the FCA's broad authority — cybersecurity enforcement. Under the Department of Justice's (DOJ's) recent Civil Cyber-Fraud Initiative, government contractors who represent their compliance with certain cybersecurity standards are being held to meet those standards or face liability under the FCA. With four recent settlements under the DOJ's initiative so far and new allegations against Penn State University, cyber-security is expected to remain at the forefront of FCA enforcement and litigation.

This intensified focus on cybersecurity began roughly two years ago when DOJ launched its Civil Cyber-Fraud initiative. Its goal is to use the FCA as a mechanism to detect and prevent suspected cyber fraud by government contractors. The initiative not only targets companies that knowingly fail to report cybersecurity breaches in a timely manner, but it also focuses on companies that misrepresent their own cybersecurity protocols in their contracts with the government. The initiative came as a result of President Biden's executive order demanding that the government strengthen its cybersecurity efforts. Deputy Attorney General Lisa O. Monaco then announced the initiative on October 6, 2021. DAG Monaco stated that the initiative is "a tool that we have to ensure that taxpayer dollars are used appropriately and guard the public fisc and public trust." DAG Monaco further warned that companies choosing "silence" by failing to report a cybersecurity breach "changes today." The initiative also seeks to ensure companies who "follow the rules" do not face competitive disadvantages.

The first major settlement under the initiative came swiftly in March 2022 against Comprehensive Health Services LLC (CHS). The Florida company, a global provider of medical support services, agreed to pay $930,000 to settle government claims that CHS falsely represented that it complied with contract requirements in providing those services at State Department locations in Iraq and Afghanistan. Although no cybersecurity breach occurred, the government alleged that, between 2012 and 2019, CHS failed to consistently store patient medical records on a secure EMR system as required under its contract.

Around the same time, Jelly Bean Communications Design LLC agreed to pay $293,771 to resolve FCA allegations that it failed to secure personal information on a federally funded health insurance website that it hosted and maintained under contract with the government. The government accused Jelly Bean of failing to provide secure hosting of the website HealthyKids.org, as over 500,000 applications submitted on this website for health insurance were hacked.

Recently, Verizon Business Network Services LLC agreed to pay $4,091,317 because of its failure to meet certain cybersecurity standards concerning its Managed Trusted Internet Protocol Service (MTIPS), which was software Verizon designed and provided to various federal agencies between 2017 and 2021. This system was intended to provide federal agencies with secure connections to the public internet and external networks but allegedly failed to meet three of the government's key security requirements. Notably, Verizon self-reported the violations to the government. Verizon then launched its own compliance review and cooperated with the government's investigation, adopting substantial remedial measures.

These settlements demonstrate that DOJ is using the FCA to enforce representations in government contracts related to cybersecurity, even when no breach has occurred. The Verizon settlement, in particular, is also an example of the benefits of voluntary disclosure and remediation of compliance failures. Rather than remaining quiet and facing a prolonged and costly government investigation, Verizon informed the Government of its investigatory findings and cooperated to remediate its cybersecurity weaknesses. Under the FCA, a company can be required to pay three

Arthur P. Fritzinger

Member

afritzinger@cozen.com
Phone: (215) 665-7264
Fax: (215) 665-2013

Calli Jo Padilla

**Member
Co-Chair, Women's Initiative**

cpadilla@cozen.com
Phone: (215) 665-6938
Fax: (215) 253-6777

Jacqueline M. Winton

Associate

JWinton@cozen.com
Phone: (215) 665-2058
Fax: (215) 665-2013

Related Practice Areas

- White Collar Defense & Investigations

times the government's loss in addition to extra penalties. However, Verizon only paid a 1.5 multiplier due to its cooperation.

Private whistleblowers are taking notice, too. Aerojet Rocketdyne, a provider of missiles and space vehicles, agreed to pay $9 million after facing allegations that it misrepresented its compliance with the government's cybersecurity requirements in various federal government contracts. A former Aerojet employee, Brian Markus, blew the whistle on Aerojet and received $2.61 million as part of his share of recovery under the initiative's *qui tam* provision. This July 2022 settlement underscores how employees are watching and are massively incentivized to come forward and report any cybersecurity violations of their employers.

A lawsuit unsealed in September shows that cybersecurity enforcement extends beyond commercial government contracts and into the academic research industry. On September 1, 2023, the U.S. District Court for the Eastern District of Pennsylvania unsealed a *qui tam* FCA lawsuit against Penn State University for failure to provide adequate cybersecurity controls for Covered Defense Information. The lawsuit, brought on behalf of the former Chief Information Officer of Penn State's Applied Research Laboratory, Matthew Decker, alleged that the university falsely certified its cybersecurity compliance with government requirements.

The allegations against Penn State show the breadth of potential FCA enforcement, particularly as the government includes cybersecurity representations and requirements in more contracts. This use of the FCA to strengthen the nation's cybersecurity infrastructure is only expected to increase. Any organization entering into a contract with the government should pay close attention to the cybersecurity protocols and requirements of the contract, partner with its Information Technology teams to ensure strict compliance with those requirements and make sure that it accurately represents its cybersecurity protocols to the government.