

Software Provider and DOJ Reach \$8.6M Settlement for FCA Case Involving Alleged Cyber Security Shortcomings

August 20, 2019 – FCA Now

by Jack Huerter

Amid increased public and government attention to cyber security, a *qui tam* plaintiff's lawsuit has resulted a large settlement for a government contractors' purported misrepresentations regarding compliance with government cyber security standards. In what is believed to be the first-of-its-kind settlement of an FCA claim premised upon cyber security misrepresentations, Cisco Systems recently agreed to pay \$8.6 million to the federal and state governments.

The case, *United States of America v. Cisco Systems*, involved allegations from a former-subcontractor whistleblower that Cisco Systems knowingly sold video monitoring technology containing security flaws to the United States, eighteen states, and the District of Columbia. See Complaint, Case No. 11-cv-400 (W.D.N.Y. May 5, 2011). According to the whistleblower, the security flaws to the video monitoring technology created a backdoor to the system, enabling a potential user to gain unauthorized access to the entire network of a federal agency, take control of or bypass an agency's physical security systems, or even allow an unauthorized user to obtain administrative access to the system to make modifications. *Id.* Notwithstanding its awareness of the security flaws, and knowing that the disclosure of the security flaws would have prevented the federal government from purchasing the video monitoring technology, the Relator alleged that Cisco Systems withheld information regarding the security flaws from multiple federal and state agencies to which it sold the video monitoring technology. *Id.*

On July 31, 2019, the federal government, fifteen states, and the District of Columbia settled the claims against Cisco Systems. Pursuant to that agreement, Cisco Systems will pay \$2.6 million to the federal government to resolve the FCA claims and approximately \$6 million to state governments to resolve similar state law fraud-in-contracting claims. Cisco framed the settlement as a "partial refund" to the governments involved, and did not explicitly admit liability. The company acknowledged that "times and expectations have changed."

Related People

- Jack Huerter

Related Capabilities

- Healthcare Enforcement & Compliance
- Government Enforcement & Corporate Investigations

The settlement may be a harbinger of more cyber security claims to come. Information security has become an increasingly prominent component of all government contracts, extending well beyond contracts in the information technology space. Government contractors will therefore be increasingly required to abide by the security standards imposed by the Federal Information Security Management Act and related regulations when selling products to the government. The recent seven-figure settlement emphasizes the government's interest in pursuing FCA actions premised upon cyber security shortcomings, and serves as a reminder to government contractors to be mindful of their cyber security compliance obligations.