On the WLF Legal Pulse

Timely commentary from WLF's blog

Washington Legal Foundation
Advocate for Freedom and Justice®
2009 Massachusetts Avenue, NW
Washington, DC 20036
202.588.0302 wlf.org

October 4, 2019

U.S. ex rel. Glenn: What We Can Learn from Cisco's Settlement of FCA Suit Alleging Cybersecurity Violations

by Stephen A. Wood

On July 31, 2019 a False Claims Act complaint was unsealed with the contemporaneous announcement that the defendant in the case, Cisco Systems, Inc., had agreed to a settlement of all claims in the matter for a seven-figure sum. The firms representing the relator touted the settlement as groundbreaking, the first ever involving a breach of information-security requirements. The action was filed in 2011 and so predated current Federal Acquisition Requirements that impose direct obligations on contractors related to cybersecurity. Nevertheless, the relator alleged that Cisco knowingly sought payment for a system that put agency security at risk. The settlement highlights the growing FCA risk that businesses face with regard to information security. In addition, this and other recent cases further reveal the compliance challenges faced by government contractors and other businesses who rely upon revenue from government sources.

The Action Against Cisco

Filed as a *qui tam* action on May 10, 2011, the complaint names James Glenn, a former employee of Cisco's Danish distributor, as relator. The action was brought on behalf of the United States as well as eighteen states and the District of Columbia under their respective anti-fraud statutes. Cisco was the sole defendant. Glenn alleges that he was fired by his employer when he complained about software defects in Cisco's products. The only publicly available pleading is the complaint, which was unsealed on the day the settlement was announced.

At issue in this case was a Cisco-manufactured video surveillance system sold by it or by distributors to state and federal governments. The Cisco Video Surveillance Manager (VSM) runs on internet protocol-based software. The VSM allowed for connection and management of multiple video cameras through a centralized server, which in turn was accessible remotely over the internet. Cisco acquired the software from another company and adapted it for use in its VSM. Relator alleges that the security flaws existed at the time Cisco acquired the software and Cisco never fixed them.

The claimed security flaws were alleged to put a user's entire information-management system at risk. Many customers, it was claimed, connected their video surveillance systems to their main computer systems through a local area network (LAN). In theory, anyone gaining unauthorized access to one video camera could access the entire computer system of a federal or state agency. This could permit a hacker, the complaint warns by way of example, to shut down an airport, or erase evidence (video or otherwise) of a crime. And because these systems were marketed to persons responsible for physical, as opposed to information, security, the flaws were less likely to ever be detected.

Stephen A. Wood is a Principal with Chuhak & Tecson, P.C. in the firm's Chicago, IL office. He is the *WLF Legal Pulse*'s Featured Expert Contributor on the False Claims Act.

Relator claims that he discovered the flaws because his employer, a Danish company called NetDesign, generally encouraged employees to test the company's products, software, and systems to identify weaknesses. As part of this effort, relator discovered these flaws in the VSM and reported them to his managers as well as Cisco. A couple of months later, relator was terminated ostensibly for financial reasons, which he suggested were pretextual given the company's strong financial performance that year. Eventually, relator made his way to law enforcement in the U.S., providing the same information regarding the security flaws he had provided to Cisco.

Relator alleged that Cisco violated a federal regulatory scheme consisting of statutes, regulations, and standards. The starting point for his theory was the Federal Information Security Management Act of 2002 (FISMA), as implemented through the Federal Acquisition Regulations.[1] FISMA required federal agencies to implement regulations pertaining to information security. The statutory text includes the following rationale: "Unauthorized disclosure, corruption, theft, or denial of IT resources have the potential to disrupt agency operations and could have financial, legal, human safety, personal privacy, and public confidence impacts. . . . In particular, there is need to focus on the role of contractors in security as more and more Federal agencies outsource various information technology functions."

Relator alleged further that the Federal Acquisition Regulations at 48 CFR § 11.102 refer procurement stakeholders to the Federal Information Processing Standards (FIPS). The FIPS in turn incorporate certain National Institute of Standards and Technology (NIST) Special Publications, in particular SP 800-53. Cisco was alleged to have violated several SP 800-53 standards, including, for example, sections AC-3 ("Access Control Enforcement"), IA-5 ("Authenticator Management"), SC-8 ("Transmission Integrity"), SC-9 ("Transmission Confidentiality"), SC-23 ("Session Authenticity"), and SI-10 ("Information Input Validation").

The Complaint asserts liability in a single count for violation of multiple sections of 31 U.S.C. § 3729 (a)(1). Similarly, the complaint contains a single count brought under each of the anti-fraud statutes of 18 states and the District of Columbia, for a total of 20 counts. Each follows the same pattern. No new facts are alleged. Cisco is claimed to have, among other things, "knowingly presented or caused to be presented, false or fraudulent claims for video surveillance software" as well as "knowingly made, used, or caused to be made or used, false or fraudulent records or statements material to false or fraudulent claims . . . ." Each count includes an allegation of conspiracy between Cisco and NetDesign, relator's employer, "and others of its partners and affiliates, to commit statutory violations," although no company other than Cisco is named as a defendant.

In response to the public announcement of the settlement, a Cisco spokesperson stated: "We are pleased to have resolved a 2011 dispute involving the architecture of a video security technology product. . . . There was no allegation or evidence that any unauthorized access to customers' video occurred as a result of the architecture." Public reports regarding the suit indicate that Cisco publicly acknowledged the problem, stopped selling the allegedly defective unit, and issued a software fix in 2013.

Analysis of the Settlement

Although the complaint isn't entirely clear, relator implies that he was responsible for bringing this issue to Cisco's attention, that it had no prior knowledge of the flaws in its VSM product. If true, it is fair to question whether Cisco would bear liability for any pre-notification conduct. An argument for liability would implicate what Cisco knew about the software before it sold the VSM and the technical difficulty required to discover the security flaws. And Cisco's failure to detect the flaws on its own would have to rise to the level of reckless disregard or deliberate ignorance under § 3729 (b)(1). Of

[1] FISMA has since been replaced by the Federal Information Security Modernization Act of 2014.

course, once on notice, Cisco could be held liable for continued sales of the allegedly defective system. Notably, the complaint contains no allegation that Cisco certified compliance, expressly or impliedly, with information-security requirements.

The amount of the settlement, approximately $8.6 million, seems relatively modest, given the number of plaintiffs involved and the likely number of sales of the video monitoring system. This was probably because no system was actually shown to have been breached, according to Cisco. In addition, contrary to the allegations that the defects rendered the system "worthless," customers no doubt received value for the systems and used them for their intended purpose, despite the claimed software defects. It is entirely possible, too, that the allegations regarding the magnitude of the risk were overstated, that although it may have been possible for a hacker to access a video camera, the likelihood of a system-wide breach was much less likely.

At the time of the filing of the Cisco complaint, the relevant regulations and standards affected contractors only indirectly. Cisco's product, it was alleged, caused agencies to be in breach of their obligations under FISMA to ensure the security of information assets (data and systems) including those provided or managed by contractors. There was no allegation that Cisco violated a regulatory or contractual term imposed directly on it. Instead, Cisco's primary failing, it seems, was selling systems after notice of defect, albeit a defect that did not necessarily prevent the product from performing its intended function. In that sense, the Cisco case is more like a run-of-the-mill defective product FCA case, where the seller knows its product is defective and fails to rectify the matter or at least inform the government. In such a light, the Cisco settlement seems less ground-breaking.

What Does the Cisco Settlement Portend?

This is not to suggest that the Cisco settlement does not serve as a forerunner of information-security enforcement and litigation. Just the opposite is likely. This is a logical consequence of our government's dependence upon technology and the internet, which in turn leads to regulation. After the filing of the Cisco complaint, the federal government issued regulations that imposed requirements on government contractors directly. In 2013, the Department of Defense promulgated 48 CFR 252.204.7012, titled "Safeguarding covered defense information and cyber incident reporting," and proceeded to amend it multiple times over the next three years, creating a moving compliance target for industry.[2] Contractors outside the defense industry must look to 48 CFR 52.204-21, similarly titled "Basic Safeguarding of Covered Contractor Information Systems." The clause imposes a set of 15 basic requirements on contractors related to information security including, for example, limiting access to authorized users, authenticating the identities of those who have access to information, and controlling physical access to systems or data.

The terms of both provisions are rather vague and broad. For example, adequate security is defined under 252.204.7012 as "protective measures that are commensurate with the consequences and probability of loss, misuse, or unauthorized access to, or modification of information." This regulation further states that contractors must "apply other information systems security measures when the Contractor reasonably determines that information systems security measures, in addition to those identified in paragraphs (b)(1) and (2) of this clause, may be required to provide adequate security in a dynamic environment or to accommodate special circumstances (*e.g.*, medical devices) and any individual, isolated, or temporary deficiencies based on an assessed risk or vulnerability. These measures may be addressed in a system security plan." Ensuring compliance with such provisions is a challenge

[2] This provision currently incorporates NIST SP 800-171, "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations" which sets forth information-security requirements and can be found at http://dx.doi.org/10.6028/NIST.SP.800-171. In 2018 NIST released a revision for SP 800-171 which includes minor editorial changes to select security requirements for controlled unclassified information (CUI), additional references and definitions, and an updated appendix that contains an expanded discussion of each CUI requirement.

and warrants contract specific clarification through communication with the agency and agreement on a specific security plan. Thus, not only must contractors be cognizant of information-security compliance and attendant FCA litigation risk, but they must ensure that they have taken steps to identify as precisely as possible what security measures are required, and if those are not met, that the relevant facts are disclosed to the governing agency.

Even this may not be enough to forestall a *qui tam* filing, however, as can be seen in *United States ex rel. Markus v. Aerojet Rocketdyne Holdings, Inc.*, pending in the Eastern District of California. Relator, former head of cybersecurity at the defendant company, alleged that the defendant failed to comply with applicable regulations, including 252.204.7012. In his complaint, he asserted two counts under the FCA: (1) that defendant committed promissory fraud in that compliance was a prerequisite to contract award, and (2) that defendant submitted false records in connection with claims for payment.[3] The former claim, if proved, is more serious because it could lead to a finding that all contract invoices were false claims. *See, e.g., United States ex rel. Marcus v. Hess*, 317 U.S. 537 (1943) (contract awarded as a result of collusive bidding renders all subsequent invoices false). Defendant moved to dismiss, mainly on lack of facts to show any material violation. In support, the defendant offered evidence that it had been in communication with the DOD regarding its cybersecurity compliance and had actually disclosed that it was not compliant. The court denied the motion to dismiss holding that the complaint alleged enough facts to establish materiality, mainly insofar as the extent of defendant's noncompliance may not have been disclosed.

Apart from federal procurement, the health care industry faces similar risk of litigation related to information-security compliance. As an example, providers and other possessors of protected health information are required to safeguard this data under the Health Insurance Portability and Accountability Act (HIPAA). Breach of these requirements through inadequate information-security measures could result not only in liability for violations of HIPAA, but also possibly under the False Claims Act were a relator to allege the submission of Medicare or Medicaid claims for payment impliedly certified compliance with applicable regulations, including information security under HIPAA. *See, e.g., United States ex rel. O'Donnell v. America at Home Healthcare and Nursing Svcs., Ltd.*, No. 14-cv-1098, 2018 WL 319319 (Jan. 8, 2018 N.D. Ill.) (denying motion to dismiss relator's claim that HIPAA violation is actionable under FCA). This was essentially the theory put forth in *Universal Health Services, Inc. v. United States ex rel. Escobar*, 136 S. Ct. 1989 (2016), where relator alleged that the defendant impliedly certified compliance with a variety of state and federal regulations by virtue of submitting claims for federal and state reimbursement.

Conclusion

The Cisco settlement and related information-security litigation reveals that any business subject to a government requirement of information security faces the possibility of litigation under the False Claims Act for violation of those requirements. Although an information-security breach would surely expose a company to greater liability, the lack of one will not insulate a company from exposure under the FCA, as was the case with the Cisco settlement. Compliance efforts must focus on these requirements, including the specification of requirements where clarity is lacking. This is likely to be an ongoing challenge for companies doing business with federal and state governments. Because technology is constantly changing, and security measures adequate one day may become obsolete the next, constant vigilance is necessary.

[3] In a third count, relator also alleged conspiracy in violation of the FCA, although this was dismissed by the district court based on the intra-corporate conspiracy doctrine, that corporations cannot conspire with related persons or entities. *See United States ex rel. Markus v. Aerojet Rocketdyne Holdings, Inc.*, 381 F. Supp. 3d 1240, 1249-50 (2019).

