wiley

ARTICLE

Escobar Increases Risk of Cybersecurity-Based FCA Litigation

Law360
July 8, 2016

Last month, the U.S. Supreme Court held in *Universal Health Services Inc. v. United States et al. ex rel. Escobar*, __ S.Ct. __, 136 S.Ct. 1989 (2016), that the implied certification theory of liability under the False Claims Act is valid, greatly increasing the types of FCA claims that can be brought against contractors. This ruling presents heightened risks for FCA liability based on a contractor's cybersecurity practices. This article discusses how the implied certification theory may open the door to increased FCA cybersecurity claims, why this area presents heightened risks for contractors, and three steps contractors can take to mitigate this risk.

Noncompliance with Contractual Cybersecurity Requirements Is More Likely to Be the Basis of an FCA Claim

Universal Health Services held that in certain instances an FCA claim may be based on noncompliance with regulatory and contractual requirements even in the absence of an express certification about those requirements to the government. Under this theory of liability, known as implied certification, the court held that "liability can attach when the defendant submits a claim for payment that makes specific representations about the goods or services provided, but knowingly fails to disclose the defendant's noncompliance with a statutory, regulatory, or contractual requirement." Id. at 1995. The court also held that "liability for failing to disclose violations of legal requirements does not turn upon whether those requirements were expressly designated as conditions of payment." *Id.* at 1996. Instead, the court determined that the focus should be on the materiality of any such omission. *Id.*

Authors

Stephen J. Obermeier
Partner
202.719.7465
sobermeier@wiley.law

Practice Areas

Civil Fraud, False Claims, *Qui Tam* and Whistleblower Actions
Government Contracts
Internal Investigations and False Claims Act
Issues and Appeals
Litigation
Privacy, Cyber & Data Governance
White Collar Defense & Government Investigations

These two holdings mean that, in theory, the government can allege that a contractor's failure to comply with cybersecurity requirements in a contract — like a clause mandating compliance with National Institute of Standards and Technology Special Publication 800-171 — could be a basis for FCA liability. That is true even where the government does not expressly condition payment on that clause and the contractor does not make an express statement about complying with NIST 800-171.

In our experience, it is unusual for contractors to expressly certify compliance with contract requirements related to cybersecurity, thus "traditional" FCA claims based on an express certification about cybersecurity have been rare. Federal agencies are, however, increasingly including cybersecurity requirements in contracts. The government (and *qui tam* relators) will no doubt argue that the implied certification theory endorsed by the Supreme Court may, under the right circumstances, reach noncompliance with these provisions.

Contractors May Be Especially Vulnerable to FCA Litigation for Noncompliance With Cybersecurity Requirements

Contractors Are Increasingly Facing Demanding Cybersecurity Requirements

Government contractors will be at increased risk of FCA liability predicated on cybersecurity lapses based on the confluence of several factors. First, contractors are increasingly bearing the burden of the federal government's attempts to improve cybersecurity. For example, U.S. Department of Defense contractors must comply with NIST 800-171, which sets out steps to protect controlled unclassified information (CUI). In addition, in August 2015, the Office of Management and Budget issued preliminary guidance that would require all contractors to incorporate certain NIST cybersecurity provisions, guidance that we expect to become finalized in the relatively near future.

Second, cybersecurity is notoriously difficult to regulate and to implement. The reality is that mature cybersecurity is constantly evolving and reacting, often requiring significant — and costly — changes to industry. To some extent, the federal government recognizes this. For example, on Dec. 30, 2015, the DOD revised its prior rule requiring implementation of NIST 800-171, allowing for flexibility in phasing-in the new baseline. *See* 80 Fed. Reg. 81472. The DOD was sensitive to the need "to provide immediate relief from the requirement to have NIST 800-171 security requirements implemented at the time of contract award," as contractors would otherwise be "at risk of not being able to comply with the terms of contracts that require the handling of covered defense information" upon contract award under the initial interim rule.

Despite some recognition of how difficult cybersecurity is to regulate and implement, the federal government is under intense pressure to respond to the massive data breaches in the private sector, and, more poignantly, at federal agencies like the U.S. Office of Personnel Management. In particular, the federal government has engaged in numerous cybersecurity "sprints." As a result, government contractors are increasingly being required to meet evolving cybersecurity benchmarks, a trend we only see accelerating.

Third, contractors are being required to undergo increasingly intensive cybersecurity assessments and penetration tests as agencies work to comply with the Federal Information Security Management Act. By their nature, assessments and penetration tests are designed to find lapses in security, which results in

documenting potential noncompliance a contractor may have with contractually mandated cybersecurity provisions, like NIST 800-171.

In the hands of the relators' bar or an aggressive U.S. Department of Justice attorney, these assessments and penetration tests could become critical evidence to demonstrate scienter. As *Universal Health Services* affirmed, "deliberate ignorance" or "reckless disregard" of the "truth or falsity of the information" is sufficient to prove scienter in an FCA case. *Id.* at 2001-2002. FCA liability could be premised on arguments that a contractor in possession of a cyber assessment or penetration test that outlines noncompliance issues is, at the least, in reckless disregard of any lapses outlined in those tests, thereby making a scienter defense more difficult.

This uncertain, fast-paced environment presents increased risk of FCA litigation. Contractors are being forced to adopt often onerous cybersecurity requirements, and they are being told to do so at a "sprint." Imperfect compliance with these requirements seems inevitable, and, especially after a cyberincident, relators' counsel — and the Department of Justice — may look to capitalize by bringing FCA claims.

Universal Health Services' Resurgent Definition of Materiality May Not Be Helpful in this Context

A criticism of the implied certification theory is that it potentially turns garden-variety breach of contract claims based on trivial noncompliance into fraud claims with the risk of treble damages.[1] The Supreme Court in *Universal Health Services* cautioned that the FCA "is not an all-purpose antifraud statute … or a vehicle for punishing garden-variety breaches of contract or regulatory violations." *Id.* at 2003. To prevent this, the court stressed that vigorous enforcement of materiality was needed.

In order to prove an FCA claim, the government or a relator must prove that a false certification is "material" to the government's decision to pay the contractor. *Id.* at 2002. In theory, materiality should differentiate between the many trivial instances in which a contractor's cybersecurity protections are not in line with a contractual requirement and the moments of true fraud where a contractor deceives the government. *Id.* ("Concerns about fair notice and open-ended liability can be effectively addressed through strict enforcement of the Act's materiality and scienter requirements. Those requirements are rigorous.")

That hope may be particularly difficult to realize in the context of cybersecurity when materiality may, in some cases, be evaluated after a data breach. The reality is that these FCA claims could be litigated with the benefit of hindsight, after a contractor's network has suffered a data breach resulting in the loss of sensitive federal information. In that context, hackers may have exploited what otherwise appeared to be a trivial or understandable cybersecurity lapse. Fairly or not, relators and the government may be positioned to exploit and unduly increase the importance and apparent materiality of that lapse in cybersecurity by arguing that the lapse caused the data breach.

In sum, contractors are facing increasing contractual requirements related to cybersecurity, they are struggling to implement those requirements, and they are required to regularly document their shortcomings in mandated assessments. On top of that, relators or the government may seek to water down *Universal Health Services*' materiality standards by bringing complaints after an incident when seemingly trivial instances of

noncompliance contribute to significant data breaches.

Contractors Should Take the Following Steps

1. Review All Statements to the Government to Eliminate "Actionable Half-Truths"

Federal circuit courts had articulated different versions of the implied certification theory, and the version the Supreme Court backed was by no means the worst one for contractors. For example, in *Universal Health Services*, the court required that in order for an FCA case to go forward on an implied certification theory, plaintiffs must prove that the contractor made "actionable half-truths."

Specifically, the court held that "the implied certification theory can be a basis for liability, at least where two conditions are satisfied: first, the claim does not merely request payment, but also makes specific representations about the goods or services provided; and second, the defendant's failure to disclose noncompliance with material statutory, regulatory, or contractual requirements makes those representations misleading half-truths."

To be sure, the concept of an "actionable half truth" lacks precise contours. Still, whatever "half truths" may eventually mean, it requires some sort of "specific representation" or affirmative statement to the government. Contractors should carefully review all of their statements to the government regarding cybersecurity to determine the potential for submitting misleading half-truths.

As one general recommendation, contractors should avoid sweeping pronouncements about their cybersecurity capabilities. For example, contractors should be wary of claiming that they are "compliant with NIST 800-171" or similar guidance. Sweeping pronouncements, as opposed to more specific and readily verifiable representations, will carry the risk of multiple interpretations.

2. Consider Informing the Government About Cybersecurity Lapses in Order to Take Advantage of the Government Knowledge Defense

Under the FCA, several circuit courts have held that a defendant can avoid liability by showing that the government was aware the defendant was submitting claims containing inaccurate or incomplete information but nevertheless accepted, or even encouraged, such claims. *United States ex rel. Ubl v. IIF Data Solutions*, 650 F.3d 445 (4th Cir. 2011); *United States ex rel. Burlbaw v. Orenduff*, 548 F.3d 931 (10th Cir. 2008); *United States ex rel. Costner v. URS Consultants*, 317 F.3d 883 (8th Cir. 2003); *United States ex rel. Becker v. Westinghouse Savannah River Co.*, 305 F.3d 284 (4th Cir. 2002).[2]

The court in *Universal Health Services* affirmed this defense, holding that government knowledge of noncompliance with regulatory or contractual requirements will likely defeat any claim that those instances of noncompliance were material. "If the Government pays a particular claim in full despite its actual knowledge that certain requirements were violated, that is very strong evidence that those requirements are not material." *Universal Health Services*, 136 S.Ct. at 2004.

Contractors who know that their cybersecurity practices fall short of their contractual requirements may consider disclosing those gaps to the government. In doing so, they could insulate themselves from claims of having made a material omission to the government. Specifically, they would be able to defeat materiality by showing that the government has actual knowledge of any less-than-perfect cybersecurity practices but made payments anyway.

3. Legal Counsel Should Lead Cyber Assessments and Penetration Tests

Contractors should have tech-savvy counsel lead any cybersecurity assessments. Computer forensic experts, appropriately, tend to focus on the negatives — what needs to be fixed, upgraded and patched. When documenting these areas for improvement, they usually are not thinking about how the documentation they are creating could be taken out of context in a future litigation or the valid reasons why certain improvements might be impractical from a business stand point.

In addition to the benefits of having cyber assessments protected by the attorney-client privilege in appropriate cases, legal counsel can make certain that a contractor's cybersecurity documentation will stand up in the harsh light of an FCA complaint after a data breach. For example, legal counsel make certain that the documentation is not just a wish list of what could be improved, but a more thoughtful analysis of what cybersecurity steps make business sense at any given time.

In addition, legal counsel can make certain that a contractor's cybersecurity documentation also includes a description of the positive steps a contractor is taking. For example, many large companies see thousands of attempted cyber attacks a day taking the form of spear phishing, malware and distributed denial-of-service attacks. Legal counsel should look to document those successes as well to create a more complete picture of a contractor's cybersecurity.

---

[1] As the court held, "If the Government required contractors to aver their compliance with the entire U.S. Code of Federal Regulations, then under this view, failing to mention noncompliance with any of those requirements would always be material. The False Claims Act does not adopt such an extraordinarily expansive view of liability." *Id.* at 2004.

[2] Interestingly, *Universal Health Services* tied the government knowledge defense to materiality, whereas several prior decisions by Circuit Courts had connected the government knowledge defense to scienter. See, e.g., *United States v. Southland Mgmt. Corp.*, 326 F.3d 669, 682 (5th Cir. 2003) ("Most of our sister circuits have held that under some circumstances, the government's knowledge of the falsity of a statement or claim can defeat FCA liability on the ground that the claimant did not act 'knowingly.'").