Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

New Tech, Old Rules: 6 Tips For Tech Cos. Managing FCA Risk

Law360, New York (March 22, 2016, 2:59 PM ET) --


Stacey M. Sprenkel


Nicholas S. Napolitan


Ian K. Bausback

When it was first enacted in 1863, the original purpose of the False Claims Act was to prosecute war profiteers who were selling sick mules and broken muzzle-loaded rifles to the Union Army. In recent years, its use has expanded to reach a broader scope of market participants — including the upstream suppliers and manufacturers of products that ultimately get purchased with federal dollars. Because the government uses technology products and services, this naturally includes tech companies. Consequently, device manufacturers, software developers and technology service providers who do not think of themselves as traditional government contractors have found themselves facing the potential for liability under the False Claims Act.

The Reach of the False Claims Act

The False Claims Act imposes civil liability when false or fraudulent "claims for payment" are presented to the government. It can reach anyone who presents a false claim to the government, as well as anyone who "causes" another company to present a false claim. It also applies to anyone who makes "a false record or statement" that is likely to influence a claim to the government, regardless of who submits that claim. Those who are held liable under the statute could face treble damages, as well as cumulative civil penalties that can reach as high as $11,000 per claim.[1] This had led to sizable recoveries: The U.S. Department of Justice recently reported recovering $3.5 billion during 2015 alone. Since 2009, it has recovered over $26.4 billion through settlements and judgments. Beyond monetary damages, a company could also face suspension and debarment from federal contracting in some circumstances.

One unique feature of the False Claims Act is that it authorizes both the attorney general and, with certain restrictions, private relators to bring civil actions. Most suits brought against tech companies are initiated by current or former employees, who file suit as relators. When a claim raised by a relator results in a settlement or a successful prosecution, the relator is entitled to a share of the government's recovery.[2]

Common Claims Asserted Against Tech Companies

The majority of recent False Claims Act suits against tech companies focus on the company's pricing practices with respect to their nongovernmental customers. To ensure that the federal government obtains reasonable prices, the government requires vendors to provide information about their pricing practices before they can do business with multiple government agencies under the Multiple Award Schedule program.[3] In the last several years, numerous tech companies have been accused of providing inaccurate and incomplete information about the pricing and discounts that they offer to their commercial customers.

One current example of this kind of suit is United States ex rel. Shemesh v. CA Inc.[4] This suit is based on allegations that a software company failed to disclose its pricing practices to the government, resulting in overpayments of more than $100 million over a 10-year period. The relator, a former employee of the software company, is alleging that the price lists that the company provided to the government were inaccurate because they failed to disclose discounts to some of the company's commercial customers, including overseas customers.

Companies can face accusations of violating the False Claims Act even if they do not sell software or services directly to the government. In particular, several tech companies that authorize independent resellers to sell their products or software have been accused of making "false records or statements material to false claims" based on information or certifications that they provide to their resellers. Resellers may incorporate such information into applications for government contracts, or may otherwise rely upon such information when dealing with government agencies. In one recent example, Samsung Electronics Co. Ltd. paid $2.3 million to settle claims that it falsely certified that its products were made in countries designated under the Trade Agreements Act of 1979. Samsung made these certifications not to the government itself, but to resellers who did business with the government.[5]

Another way that tech companies can find themselves embroiled in False Claims Act litigation is by merging with or acquiring companies that have done business with the government in the past. When a company acquires a vendor that is subject to False Claims Act liability, the company also acquires the liability. For instance, in 2013, Axway Inc. spent $6.2 million to settle allegations that arose from the alleged failure of Valicert Inc. to fully disclose its pricing when it entered into a software licensing and service agreement in 2001. Axway faced liability as a successor in interest to Valicert. Axway had merged with a third company, Tumbleweed Communications Corporation, that had merged with Valicert back in 2003. Neither Axway nor Tumbleweed had corrected the pricing as required by the agreement.[6]

The global nature of the technology industry also poses unique False Claims Act risks. Recently, several cases have arisen in which tech companies are accused of violating the False Claims Act by using engineers and employees who are ineligible to perform certain work because of their overseas location, insufficient security clearance, or other factors. As just one example, last year the information technology service provider Global Computer Enterprises paid $9 million to settle allegations that it violated the False Claims Act by using engineers who were prohibited from working on certain government contracts due to their citizenship status.[vii] Such claims can arise even against companies that are scrupulous about their own hiring practices, e.g., if they fail to screen the practices of their subcontractors.

Ultimately, companies can be accused of violating the False Claims Act based on any conduct that can be construed as less than fully forthcoming, such as overbilling or including hidden charges in bills. This can

also include instances where products or software do not meet warranties or representations about their features or performance. Where government funds are involved, the kinds of conduct that might normally result in a run-of-the-mill commercial contract dispute has the potential to become a large-scale federal case.

Six Ways to Control or Reduce Your Company's False Claims Act Exposure

The scope of the False Claims Act, and associated harsh penalties, can be daunting for companies that do not perceive themselves as government contractors. This is especially true for tech companies, many of which do not yet have the well-developed compliance infrastructure that defense contractors and government-facing companies have developed over decades. Here are six things that tech companies with government customers or end users can keep in mind to reduce their potential exposure:

1. Maintain Internal Price Transparency

It is important to develop and maintain internal systems that can keep track of pricing, discounts, and rebates offered to all of the company's customers, so that the company can generate accurate and up-to-date reports about pricing arrangements if it is called upon to do so. Once such systems are in place, it is equally important to establish practices that ensure that all relevant transactions go through this system, so that the company's practices are consistent with its pricing obligations to government customers. This is not only important for customers who are contracting directly with the government — it is also important for companies whose authorized resellers might rely on such information when dealing with the government.

2. Know Your Business Partners

If you are relying on information generated by a business partner in dealing with the government, or if you are subcontracting certain work that federal money is paying for, it is important to do a reasonable amount of diligence into your partner's relevant practices. Relators and the government can use circumstantial evidence to argue that any incorrect information that gets submitted to the government was a "knowing" misstatement. Moreover, relators and the government can establish liability without actual knowledge of wrongdoing, if they can support a showing that the company acted in deliberate ignorance or with reckless disregard for the truth.[8]

3. Have Systems in Place for Listening to and Vetting Concerns Raised by Employees

As noted above, the majority of recent False Claims Act suits against tech companies are initiated by employees and former employees. Having a robust system for vetting concerns, and for promptly taking appropriate steps to correct any errors or omissions, can help you identify potential problems before they turn into a federal case. It can also catch errors before they produce years' worth of alleged false claims (which is important because the government typically argues that each separate claim can be the basis for a separate $11,000 civil penalty). Moreover, having a system in place for documenting that an employee's complaints were taken seriously can support the company's position in litigation, and show that the company acted reasonably and without any knowing misconduct.

4. Don't Forget the States

The federal government is not the only government entity that uses technology products and services — and the federal False Claims Act is not the only false claims act. Most states, and some municipalities,

have their own false claims statutes or codes. Most of these include provisions for double or treble damages, as well as the potential for aggregate civil penalties. Business with state and local governments can therefore present the same kinds of issues as business with the federal government.

5. Know the Statutory, Regulatory and Contractual Requirements Applicable to the Products and Services That You Provide

Whenever your business has a nexus with government dollars, familiarity with the rules of engagement is especially critical. Developing in-house expertise, or building relationships with outside experts who know and understand your business, can reduce exposure and save you grief in the long run.

6. Have a Plan

If your company suspects that a violation of the False Claims Act has occurred, if a violation is reported by an employee, or if your company receives a government inquiry, you will need to act promptly. Consider what appropriate steps may be required, including potentially engaging outside counsel, to investigate issues that might arise and to put in place appropriate remedial steps.

Whether the government is a customer or a downstream end user, False Claims Act exposure has become a cost of doing business. It is important that companies understand this exposure, and take whatever steps are possible to reduce it.

—By Stacey M. Sprenkel, Nicholas S. Napolitan, and Ian K. Bausback, Morrison & Foerster LLP

Stacey Sprenkel is a partner and head of the litigation department in Morrison & Foerster's San Francisco office. Nicholas Napolitan and Ian Bausback are associates in the firm's San Francisco office.

[1] 31 U.S.C. § 3729(a).

[2] 31 U.S.C. § 3730(b)-(c).

[3] Services Administration in order to sell their products and services to various government agencies at pre-negotiated prices and enter into blanket purchase agreements. Government contracting officers are directed to compare the offered price with "any combination of discounts and concessions offered to commercial customers," and "differences between the MAS solicitation and commercial terms and conditions . . . ." 48 C.F.R. § 538.270(c). In addition, companies often have a duty to keep the government apprised of pricing changes to its commercial customers during the course of contract performance. See, e.g., id. §§ 538.272, 552.238-75.

[4] 89 F. Supp. 3d 36 (D.D.C. 2015).

[5] Dep't of Justice Press Release, Samsung Electronics America Agrees to Pay $2.3 Million to Resolve False Claims Act Allegations, Aug. 19, 2014, https://www.justice.gov/opa/pr/samsung-electronics-america-agrees-pay-23-million-resolve-false-claims-act-allegations.

[6] Dep't of Justice Press Release, Axway, Inc. Agrees to Pay $6.2 Million to Resolve False Claims Act Allegations Related to GSA Multiple Awards Contract, Oct. 28, 2013, https://www.justice.gov/usao-md/pr/axway-inc-agrees-pay-62-million-resolve-false-claims-act-allegations-related-gsa-multiple.

[7] Dep't of Justice Press Release, IT Software Services Contractor and Its President Agree to Pay $9 Million to Settle Civil False Claims Act Allegations, May 7, 2015, https://www.justice.gov/usao-edva/pr/it-software-services-contractor-and-its-president-agree-pay-9-million-settle-civil.

[8] 31 U.S.C. § 3729(b)(1).