October 7, 2015

LAW BUSINESS TECHNOLOGY
BUSINESS TECHNOLOGY LAW
TECHNOLOGY LAW BUSINESS
THE RECORDER
daily at www.therecorder.com
An ALM Publication

Tech Firms Targeted Under False Claims Act

Winston Y. Chan and John D.W. Partridge,
Gibson, Dunn & Crutcher

As start-up technology companies mature, some begin to contract with government entities. Along with these potentially lucrative contracts come significant risks under the federal False Claims Act and analogous state laws, which impose liability on companies that defraud governmental programs. Indeed, several recent settlements running into millions of dollars confirm that the government and private whistleblowers alike actively target technology companies under the FCA.

Although the FCA is best known as the basis for multimillion- (and occasionally billion-) dollar settlements involving alleged health care and defense procurement, an analysis of FCA actions over the last decade indicates that technology and communications companies are also frequent targets of FCA government investigations and qui tam whistleblower suits. Since 2005, the government and whistleblowers have secured approximately $1.2 billion from settlements with technology and communications companies. Just this summer, cloud-computing provider VMware and its contractor, Carahsoft, settled an FCA investigation for $75.5 million. This settlement—and an ongoing suit against Symantec seeking more than $145 million—underscore the potential FCA exposure that emerging technology companies confront.

VMware and Carahsoft's $75.5 Million FCA Settlement Is the Largest by a Technology Company in More Than Three Years

The VMware and Carahsoft settlement, announced by the Department of Justice in June, illustrates the special obligations that accompany contracts between information technology providers and the government. VMware contracted with the General Services Administration under the agency's Multiple Award Schedule. The MAS Program enables contractors to sell to many government end users under a central contract, but obligates contractors to disclose their pricing policies and practices. The government accused VMware and Carahsoft of concealing pricing information, such as discounts offered to commercial customers, and thereby allegedly overcharging the government for software and related products. Notably, a qui tam complaint filed by a former VMware executive appears to have triggered DOJ's investigation.

Symantec Faces Potential FCA Liability for Alleged Violations of MAS Program Disclosure Requirements

In September, a federal judge granted in part and denied in part Symantec's motion to dismiss an FCA complaint filed by the United States, California, Florida and a whistleblower (on behalf of New York). *United States ex rel. Morsell v. Symantec Corp.*, No. 12-00800, 2015 WL 5449795 (D.D.C. Sept. 10, 2015). Based on the allegations of the whistleblower, a former Symantec employee who managed the GSA contract, the complaint asserted that Symantec failed to disclose more favorable pricing terms and misrepresented the discounts it offered on its software. The court concluded that the United States pleaded sufficient details to survive Symantec's motion to dismiss the FCA claims, but dismissed, without prejudice, the state law claims. According to the court, the complaint adequately alleged that Symantec's implied certifications of compliance with various price disclosure

requirements (and other inaccurate statements regarding pricing) were false (and material to the government's contracting decisions).

According to Symantec's SEC filings, the government's initial analysis of actual damages was $145 million. As a result of the potential exposure associated with the *Morsell* case, Symantec had accrued a contingent liability of $25 million even before the court's order.

The Government Recovered Approximately $1.2 Billion in FCA Actions Targeting Technology and Communications Companies During the Past Decade

As the VMware and Symantec matters demonstrate, the rewards of government contracting come with significant risks. Data regarding FCA actions against technology firms during the past decade bears this point out. Indeed, despite the VMware's settlement's magnitude, it is only a small fraction of the approximately $1.2 billion in FCA settlement dollars collected from technology and communications companies from 2005 through July 2015. The cases underlying this haul hinge on several theories of FCA liability.

Allegedly Improper Pricing in GSA Contracts

Approximately $675 million (or 56 percent) of the total recoveries in these FCA matters resulted from settlements involving pricing allegations similar to those leveled against VMware and Symantec. Those FCA resolutions include:

• Oracle's 2011 agreement to pay $199.5 million to settle an investigation premised on allegations that the company failed to disclose sales practices and commercial discounts for software licenses and technical support.

• Cloud-computing company EMC's 2010 agreement to pay $88 million to resolve allegations that it failed to conduct a price comparison to ensure that the government received the lowest price provided to the company's commercial customers.

• NetApp and NetApp U.S. Public Sector's 2009 agreement to pay $128 million (a then-record sum in a case alleging GSA contracting fraud) to resolve allegations that the companies failed to disclose discounting policies, standard pricing practices, and deviations from those practices.

Alleged Kickbacks

Accounting for approximately $172 million (or 14 percent) of the recoveries, the next largest category of settled FCA actions over the past decade involves alleged kickback arrangements between IT providers, consulting firms and other contractors that purportedly influenced government purchasing. For example, Accenture paid $64 million in 2011 to resolve allegations that it received kickbacks in return for recommending hardware and software to the government, fraudulently inflated prices and rigged bids in connection with federal IT contracts.

Alleged Overbilling and Unallowable Costs

A third category involves allegations of overbilling during the performance of government contracts, ranging from logging extra hours to masking overcharges through more sophisticated schemes. These types of FCA matters comprised $135 million (or 11 percent) of settlements against technology and communications companies over the past ten years. For instance, in 2013, CA Technologies agreed to pay $11 million to resolve allegations that it charged government customers twice for maintenance services associated with its software products in the period between ordering a renewal and the end of their current plan.

Other Allegedly False or Fraudulent Schemes

In addition to the categories set forth above, the government has targeted a broad spectrum of other conduct under the FCA—and recovered another $206 million in doing so (or 17 percet of FCA settlements involving technology or communications companies since 2005). For example:

• In 2012, Lucent Technologies World Services agreed to pay $4.2 million to settle allegations that it submitted misleading testing certifications to the Army in connection with the design, construction and modernization of Iraq's emergency communications system.

• From 2005 to 2010, the government recovered more than $25 million from companies for alleged fraud involving the E-Rate Program, which provides funding for schools and libraries to purchase computer hardware and Internet services. E-Rate is administered with money from the Universal Service Fund, which collects mandatory contributions from telecommunications carriers. Notably, the Fifth Circuit recently cast doubt on FCA claims relating to the E-Rate Program, concluding that despite the United States' regulatory interest in the program, it has no financial stake in its fraudulent losses because the program funds are "untraceable to the United States Treasury." *United States ex rel. Shupe v. Cisco Sys.*, Inc., 759 F.3d 379, 385 (5th Cir. 2014).

Conclusion

As these FCA resolutions demonstrate, DOJ and other federal agencies are attuned to allegations of fraud in connection with the sale of hardware, software or other technology products or services to governmental entities. The recent VMware and Symantec actions confirm that this longstanding scrutiny is unlikely to abate soon. Accordingly, technology companies interested in tapping into the $80 billion in annual U.S. governmental spending on IT should be mindful that the government will aggressively pursue any alleged misconduct.

In Practice articles inform readers on developments in substantive law. Contact Laurel Newby with submissions or questions at lnewby@alm.com.

Winston Chan, a partner in Gibson Dunn's San Francisco office and a former federal prosecutor, and John Partridge, an associate in Gibson Dunn's Denver office, counsel clients on a range of government investigations and have particular expertise in FCA matters.