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

Aveta And The Use Of Confidential Info In FCA Cases

Law360, New York (July 19, 2016, 11:44 AM ET) --

In a recent case in the District of Puerto Rico, United States ex rel. Valdez v. Aveta Inc., et al., No. 15-cv-01140-CCC (D.P.R.), the former president of Puerto Rican-based managed health care provider Aveta Inc., Jose Valdez, alleged that the health care company submitted as much as $350 million in false claims to the government through the Medicare Advantage program by manipulating risk adjustment scores. Valdez's claims largely rest on more than 26,000 documents he (allegedly inadvertently) failed to return to the company after his termination, in violation of his nondisclosure agreement. Aveta claims that many of the documents are confidential or subject to the attorney-client privilege.


James M. Koukios


Rachael K. Plymale

In a pre-discovery motion requesting return of the documents, Aveta argued that Valdez's actions violated the Federal Rules of Civil Procedure's discovery procedures, including protections for applicable privileges and unresponsive documents, and that retaining the information post-termination was wrongful. Valdez disagreed, citing precedent allowing for use of confidential information in qui tam actions so long as that information was obtained through lawful means, which he claims he did in the course of his employment as company president. Further, according to Valdez, enforcing the confidentiality agreement and requiring him to return the documents would be contrary to public policy as it would preclude him from pursuing his fraud claim on behalf of the government and allow companies to limit contractually their liability for fraud against the government.

Although the court has yet to resolve the issues in Aveta, the case highlights several issues surrounding the use of privileged and confidential information by both plaintiffs and the government in False Claims Act suits. Much to the dismay of contractors like Aveta, the government and relators may be able to utilize confidential or privileged information in the course of investigating and prosecuting false claims. Accordingly, companies should take precautions to protect their information, including by implementing a strong compliance and reporting program, properly labeling privileged and confidential information, and executing enforceable nondisclosure agreements.

Confidential Information

Plaintiffs sometimes obtain confidential information through "self help" discovery — the process of gathering information in anticipation of litigation outside the formal discovery process — as the relator in Aveta appears to have done. Such "self help" may include failing to return company documents after termination or, more nefariously, searching for and stealing company information not otherwise in the

relators' possession to support litigation claims. Although seemingly a violation of the Federal Rules of Civil Procedure, courts do not always reject self-help discovery. However, the use of self-help discovery may expose a relator to counterclaim liability or, in some instances, even criminal liability.

The whistleblower provisions in the False Claims Act protect only lawful acts. Where confidential information is lawfully obtained, public policy concerns allow for protection of the relator and use of the information by the government in its investigation, even if the information was obtained in violation of a nondisclosure agreement — a sore spot for government contractors. As argued by relator's counsel in Aveta and upheld by several courts, the public policy in favor of protecting taxpayers means that nondisclosure agreements are typically not enforceable to prevent disclosure of fraud to the government. Thus, violating a nondisclosure agreement by taking confidential information relevant to fraud allegations may not be wrongful for purposes of the False Claims Act. Some courts, however, do at least draw the line between disclosure to the government, which may be lawful for public policy reasons, and disclosure to third parties, which remains in violation of an enforceable nondisclosure agreement.

Self-help discovery that amounts to pure theft of confidential information, on the other hand, may violate, among other things, trade secret laws or the federal Computer Fraud and Abuse Act. Under these circumstances, such conduct would likely not constitute a protected activity, and the whistleblowers could face civil liability for monetary damages via a counterclaim or even criminal liability in especially egregious cases. A company wishing to pursue a counterclaim must, however, be cautious. Although some courts have recognized these counterclaims as a necessary counterbalance to protect contractor rights in the face of aggressive litigation by relators seeking a share of the government's damage award, others have deemed the act of filing a counterclaim to be itself a retaliatory act in violation of whistleblower protections.

Despite the penalties relators may face for their misconduct, some courts have held that the public policy in favor of combating fraud against the public fisc allows the government to use wrongfully obtained confidential information, so long as the government did not encourage or direct the relator to undertake the wrongful or unlawful actions (which could violate the Fourth Amendment's prohibition on warrantless searches and seizures). For example, in United States ex rel. Ruhe v. Masimo Corp., 929 F.Supp.2d 1022 (C.D. Cal. 2012), the Central District of California denied motions to dismiss and to strike brought by a defendant that claimed that the relators had based their fraud allegations on confidential information stolen from the company in violation of their nondisclosure agreement. The court held that the relators' taking and publication of documents related to the alleged fraud "was not wrongful, even in light of nondisclosure agreements, given the strong public policy in favor of protecting whistleblowers who report fraud against the government." The court further stated that "the strong public policy would be thwarted if [the company] could silence whistleblowers and compel them to be complicit in potentially fraudulent conduct" and noted that the Ninth Circuit "has stated that public policy merits finding individuals such as Relators to be exempt from liability for violation of their nondisclosure agreement."

Privileged Information

Privileged information is afforded significantly greater protection than confidential information in the False Claims Act context. Unlike confidential information, privileged materials are protected from discovery in nearly all contexts under the Federal Rules of Civil Procedure. The policy of protecting the attorney-client privilege — the importance of which is well established in federal courts — weighs heavily against policy interests in combating fraud. Courts are far less willing to allow privileged

information, whether obtained lawfully or not, to be relied upon by relators.

Whistleblowers in wrongful possession of privileged information may not only be barred from relying on it, but may also be required to return it. Although not a False Claims Act case, Burt Hill Inc. v. Hassan, No. CIV. A. 09-1285, 2009 WL 4730231 (W.D. Pa. 2009) serves to illustrate the potential consequences of improperly utilizing privileged information. The case involved allegations of misappropriation and breach of contract between the plaintiff company and defendant former employees. At issue were manila envelopes of attorney-client privileged documents that had been allegedly anonymously provided to the defendants. Rather than return the documents upon discovered, the defendants sought to rely upon them in pursuit of their defense and counterclaims. In response to the plaintiff's protests, the court not only prohibited use of the information in the proceedings, but ordered that the information be returned to the plaintiffs and all copies in the defendant's possession be destroyed. In certain contexts, the government has taken steps to discourage whistleblowers from providing it with privileged materials. For example, the U.S. Securities and Exchange Commission's Dodd-Frank Act whistleblower rules prohibit monetary awards — similar to the relator's share in the False Claims Act context — for whistleblowers whose original knowledge of fraud stems from privileged information. The relator's counsel must also be especially diligent when dealing with potentially privileged information, as review and disclosure of privileged information by the relator's counsel may result in their ultimate disqualification from the case.

Restrictions on the government's use of privileged information may be more relaxed than in the context of a private litigant. In United States v. Warshak, 631 F.3d 266 (6th Cir. 2010), for example, the U.S. Court of Appeals for the Sixth Circuit held that the "fruit of the poisonous tree" doctrine does require suppression of evidence derived from evidence protected by a testimonial or evidentiary, as opposed to constitutional, privilege or in the absence of compelled testimony. As a result, under certain circumstances, the government may be able to use privileged information supplied by a relator to pursue leads and build a case. Nevertheless, the U.S. Department of Justice often takes precautionary steps to prevent prosecutors and agents investigating a case from being exposed to potentially privileged information. For example, the DOJ regularly implements "taint" or "filter" teams to review for privilege emails and other documents received from whistleblowers or via a search warrant. Indeed, in Warshak, the government appears to have used a methodology for screening data acquired during an office search and an email search for privileged information.

Importantly, protections for privileged information apply only where the privilege has not been waived. Pleading a state-of-mind defense, i.e., that the company did not believe it was violating the law or similar claims, may result in a waiver of privilege in order to review that defense. Contractors and counsel alike should therefore thoroughly evaluate the potential benefits and detriments of raising such a defense.

Best Practices

A contractor seeking to maximize its protection of confidential and privileged information should consider various steps. First, contractors should implement a robust internal reporting system to reduce the likelihood that a whistleblower will report suspected wrongdoing outside the company. By emphasizing a culture of ethics and compliance, establishing and publicizing multiple avenues for concerned employees to report suspected wrongdoing internally, enforcing a strict non-retaliation policy, and conducting responsive investigations, companies may head off qui tam relators before they reach the courthouse and thereby avoid these complicated issues. Second, to guard against inadvertent disclosure, or to maximize the chances that information will not be used in a lawsuit if disclosed,

contractors should diligently implement systems to mark confidential and privileged information. These marked materials should also be stored in a manner that reflects their privileged or confidential nature — for example, in electronic files marked “privileged” and maintained in password-protected files off of shared servers. Employees should be trained on compliance with these policies and procedures.

Contractors should also review their nondisclosure or confidentiality agreements. Those agreements may provide valuable recourse (in at least some jurisdictions) against bad actor relators and provide an avenue for seeking return of information prior its use by a potential whistleblower. Caution is warranted, however. Publicly traded companies must review their standard confidentiality agreements and related policies in light of the SEC’s 2015 cease-and-desist order against KBR Inc. There, the SEC faulted the company for including language in its nondisclosure agreements that potentially penalized employees who failed to obtain authorization from the company’s legal department prior to disclosing corporate misconduct to the government.

Conclusion

The Aveta case provides a recent example of the complications that can arise when a former company insider becomes a qui tam relator. Given the potential limitations on a company’s ability to retrieve privileged and confidential information after the material has been made available to the government, companies should take steps to encourage employees to report suspected wrongdoing internally and to protect information through proper labeling and storage and by executing enforceable nondisclosure agreements. Meanwhile, companies and their counsel should monitor the Aveta case to see how the court resolves these issues.

—By James M. Koukios and Rachael K. Plymale, Morrison & Foerster LLP

James Koukios is a partner in Morrison & Foerster's Washington, D.C., office and former senior deputy chief of the Fraud Section in the Criminal Division of the U.S. Department of Justice. Rachael Plymale is an associate in the firm's Washington office.