An ALM Publication

THE AMERICAN LAWYER

THE AM LAW LITIGATION DAILY

Get Ready for New Waves of FCA Activity in 2020

By Douglas Baruch, Meredith Auten, Zane Memeger and Jennifer Wollenberg
January 6, 2020

As we enter a new decade of False Claims Act enforcement, there is scant evidence of any marked slowdown in either the volume of FCA cases or the opportunities for new and expansive theories of FCA liability.

Traditional FCA cases targeting the healthcare, defense, and government contractor communities are likely to continue apace, even as courts continue to grapple with the meaning of Escobar, the Justice Department flexes its dismissal authority muscles in qui tam cases, and parties debate the propriety of statistical sampling. But amidst these ongoing themes, the next waves of FCA activity—both at the federal and state levels—are building and signaling even more potential exposure and active litigation. We highlight four emerging trends here.

FCA cases arising out of antitrust investigations

Over the years, there have been relatively few significant FCA cases based on alleged collusive activity among government contractors. The Gosselin case, involving alleged bid rigging among freight forwarders handling the movement of military household goods, and the South Korea fuel supply investigations, were notable antitrust matters, resulting in more than $150 million in FCA liability. See U.S. ex rel. Bunk v. Gosselin World Wide Moving, N.V., 741 F.3d 390 (4th Cir. 2013); U.S. v. GS Caltex Corp., No. 2:18-cv-1456 (S.D. Ohio).

But the quiet period in this space is likely to end soon. The Justice Department's newly announced Procurement Collusion Strike Force—led by the Antitrust Division in partnership with 13 U.S. Attorney offices and multiple federal law enforcement agencies—will target collusive activity in public procurements, using all available criminal and civil tools at their disposal, including the FCA.

Photo: Courtesy Photo

Morgan Lewis partners lef to right: Douglas Baruch, Meredith Auten, Zane Memeger, and Jennifer Wollenberg

One expected referral source for this new Strike Force will be qui tam relators, who—believing such referrals will find a receptive audience—will seek to leverage and capitalize on the government's renewed and coordinated focus on antitrust violations involving federal and even state procurements. All of the necessary elements are in place to generate an influx of FCA activity based on antitrust violations.

FCA cases alleging non-compliance with cybersecurity requirements

Most companies are well aware of the risks they face from hackers, theft of intellectual property, and data privacy breaches, and have built appropriate defenses. But as cyber threats mount, so does the likelihood that companies doing business with the government will face liability under the FCA for failure to adhere to an ever-growing and myriad set of federal cybersecurity compliance requirements.

For instance, for the past two years, Federal Acquisition Regulation clause 52.204-21 has been incorporated into many government contracts, mandating that contractors implement and maintain certain basic information security protocols. DFARS clause 252.204-7012 imposes similar requirements on certain contractors. Comparable regulations have been in place in the healthcare arena

for even longer, following passage of the Health Information Technology for Economic and Clinical Health Act (HITECH Act). Other federal and state agencies are mandating cybersecurity compliance protocols as well.

The "knowing" false certification of compliance with clear cybersecurity regulations or contract requirements carries significant risks in terms of FCA liability (even though many of these requirements use general or ambiguous language). For instance, advocating an inducement fraud theory, qui tam relators already have argued that contractors who misrepresented cybersecurity compliance at the time of contract award are liable under the FCA for all invoices generated under the contract. See U.S. ex rel. Markus v. Aerojet Rocketdyne Holdings, Inc., 381 F. Supp. 3d 1240 (E.D. Cal. 2019).

Given the prevalence of express and implied false certification theories of FCA liability, significant FCA settlements based on certain HITECH non-compliance, and the fact that recent cybersecurity non-compliance allegations have survived dismissal challenges in federal court, it is easy to envision both qui tam lawsuits and affirmative enforcement activity by the Justice Department in this area.

Renewed emphasis on "reverse" false claim liability

The FCA's so-called "reverse" false claims provision, 31 U.S.C. § 3729(a)(1)(G), which imposes liability for making false statements material to an obligation to pay money to the government (as opposed to claiming money from the government), has been gathering steam for some time and is being used to target companies that do not do business directly with the government.

One type of reverse false claim that has drawn the attention of the qui tam plaintiffs' bar arises in the "Customs" arena. A typical allegation is that an importer mismarked the country of origin of goods or misreported items being shipped into the United States in a manner that avoids U.S. duties. See, e.g., U.S. ex rel. Vale v. Selective Marketplace, Ltd., 2:17-cv-00380 (D. Me.).

These types of allegations not only have the potential to generate substantial FCA penalties, given the number of shipments, but they also are particularly attractive to competitors who, as qui tam relators raising such claims, not only have the ability to gain a business advantage but also as a means to generate income. Claims even have been brought by "professional" qui tam relators conducting their own investigations and relying on sampling methodologies to allege reverse false claims. E.g., U.S. ex rel. Customs Fraud Investigations v. Victaulic Co., 839 F.3d 242 (3d Cir. 2016). This aspect of FCA enforcement is fertile ground for increased activity.

Expect more state enforcement

While most of the case law and discussion has focused on the federal FCA, and deservedly so given the $60 billion in recoveries since the 1986 amendments to the FCA, the fact remains that more than 30 states, plus the District of Columbia and several municipalities, have their own false claims statutes. While most are patterned after the FCA, others have significantly broader reach, including allowing claims based on violation of tax laws.

To date, state false claims enforcement has focused primarily on healthcare-related claims and the causes of action often are brought in the same federal FCA suit and arise out of the same underlying conduct that forms the basis for the federal FCA claims. But there are signs that qui tam relators are focusing on state false claims act suits as stand-alone state cases both inside and outside of the healthcare arena.

For instance, a number of recent state suits have focused on financial institutions' alleged "reverse" false claim liability for failure to comply with state escheatment laws. Other suits, sometimes brought by competitors, claim that companies selling goods in a state have failed to collect sales tax on their transactions. And, as noted above, the public procurement focus of the DOJ Strike Force would apply equally to bid rigging or collusive activity in state government procurements. Expect to see more state and municipality based false claims enforcement and claims in the coming year.

Douglas Baruch, Meredith Auten, Zane Memeger and Jennifer Wollenberg *are partners at Morgan, Lewis & Bockius.*