Whistleblower Watch
A quarterly update on FCA Enforcement and Qui Tam Litigation

Whistleblower Watch is a comprehensive source for all False Claims Act (FCA) news and information. Every quarter, Cozen O'Connor will provide in-house counsel and compliance professionals with a summary of the most notable FCA enforcement actions, settlements, and legal trends, as well as an in-depth look at emerging and significant FCA-related issues. Subscribe to stay on top of these changes and find out how they may affect you.

Recent FCA Settlements and Enforcement Actions

Medicare Advantage Audits Carry FCA Risk (Eastern District of Pennsylvania)

Private health insurer, CIGNA, agreed to pay $172 million to settle civil claims under the FCA arising principally from a Medicare Advantage audit the company performed. The audit examined certain diagnostic codes that determine the monthly reimbursement CIGNA received from Medicare for each beneficiary. The Government alleged that CIGNA's audit resulted in the addition of diagnostic codes that were unsupported by the patient medical records, and that CIGNA failed to remove erroneous diagnostic codes that would have been found during the audit. Insurers should take note of this settlement when considering any audit of Medicare Advantage programs.

Laboratory Commission Payment to Recruiters Used as Kickbacks (Eastern District of Texas)

A recent settlement by a former hospital finance chief and three physicians highlights the pitfalls of paying commissions to recruiters. On December 5, 2023, the four individual targets of a *qui tam* action agreed to pay $880,000 to settle claims that they accepted or knew of bribes in exchange for referring tests to the pathology laboratory, True Health Diagnostics, LLC. The Government claimed that True Health had paid commissions to recruiters, which were then used to bribe the defendants, using a Managed Service Organization as the middle man. The settlement highlights the reach of the Anti-Kickback Statute and the False Claims Act to prohibit commission payments that find their way to referring physicians.

Device Manufacturer Settles Claims Related to False Billing Advice (District of New Jersey)

On December 18, 2023, BioTelemetry Inc. and its subsidiary, LifeWatch Services, Inc., agreed to pay more than $14.7 million to settle civil claims that they encouraged clinics and providers to submit false claims for cardiac monitoring services. Defendants manufactured and sold a cardiac monitoring device capable of performing three different types of heart monitoring services, each reimbursable at different rates. The Government claimed that the defendants caused physicians to bill for the most expensive type of monitoring, even when medically unnecessary. The settlement highlights the importance of compliant marketing and the risks that device manufacturers face in providing billing advice to physicians who use their devices.

Cancer Center Self-Reports False Claims Related to Research Studies (Middle District of Florida)

On January 4, 2024, the H. Lee Moffitt Cancer & Research Institute Hospital agreed to pay $19.5 million to resolve self-reported violations relating to billing federal healthcare programs for clinical research studies that were ineligible for reimbursement. The settlement is one of the largest under the new Voluntary Self-Disclosure policy implemented by the Department of Justice (DOJ) last year.

Arthur P. Fritzinger
Member

afritzinger@cozen.com
Phone: (215) 665-7264
Fax: (215) 665-2013

Calli Jo Padilla
**Member
Co-Chair, Women's Initiative**

cpadilla@cozen.com
Phone: (215) 665-6938
Fax: (215) 253-6777

Related Practice Areas
- White Collar Defense & Investigations

When Moffitt discovered the false claims, it reported them to the Government and implemented several new internal policies to ensure future compliance. While Moffitt was required to reimburse the Government for the false claims, it was able to secure a non-prosecution agreement and avoid the imposition of penalties.

Legal Trends and Insights

An Increase in FCA Claims Against Schools

The education industry is highly regulated and receives substantial federal funds, making it a prime target for FCA enforcement actions. Until recently, however, the Government and *qui tam* plaintiffs mostly targeted for-profit schools. That trend is changing, as exemplified by Stanford's agreement last October to pay nearly $2 million to resolve allegations that it failed to disclose foreign funding sources when applying for research grants. Additionally, schools face FCA risks related to cybersecurity, medical and scientific research facilities, and other representations made in applications for federal funding. For additional examples of this growing trend, check out articles here, here, and here.

Reverberations from Justice Thomas's Dissent in *Polansky*

Last year, the Supreme Court upheld the Government's right to seek dismissal of an FCA action over a relator's objection, even after the Government previously declined intervention. Justice Thomas filed the only dissent, where he questioned whether the Constitution prohibited a relator from continuing with an FCA suit at all after the Government declined intervention. According to Justice Thomas, allowing a private party to proceed after declination may violate the "take care" clause of Article II, which provides enforcement authority to the executive branch. We expected that FCA defendants would advance this argument in an effort to dismiss claims the Government has declined to pursue, and Flour Corp. did just that in a *qui tam* action pending in the District of South Carolina. Read more about that case here. We will be following this trend to see if Justice Thomas's comments persuade the lower courts.

a deeper dive

Are You Sure You're Secure? DOJ's Cyber-Fraud Initiative and Heightened FCA Enforcement.

Recently, the False Claims Act has become a critically important tool for enforcing cyber-security policies in government contracting. Failures to comply with contractual cyber-security obligations can lead to false claims act prosecutions that seek to recoup all government funds paid as part of the agreement. Read more about this growing and important trend here.

Generative AI and Government Contracting

As DOJ has increased its cyber-security enforcement, generative artificial intelligence tools are promising to complicate both compliance and oversight. These tools are commonly used for drafting proposals, setting price, or predicting risks. For an analysis of the risks these tools pose under the FCA, we suggest Bloomberg's coverage here.