wiley

ALERT

Artificial Intelligence, the False Claims Act, and the Public Disclosure Bar

November 14, 2023

This article was originally published in Law360 on November 8, 2023 and can be found here.

As artificial intelligence continues to gain widespread acceptance, it is no surprise that the federal government is paying attention. As of 2020, 45 percent of government agencies were already considering the possibility of using AI tools. In 2022, Congress enacted the AI Training Act, which directed government agencies to examine the advantages of using AI. And just last week, President Biden issued a sweeping executive order providing guidelines for the use of AI.

One potential area where the government is likely to use AI is in the context of detecting fraud. But the potential for AI to detect government fraud is not limited to government agencies. There is also the potential that individuals can use AI to analyze large amounts of information, detect fraud, and bring False Claims Act (FCA) lawsuits. The use of AI tools in this context poses complicated questions, including how the use of publicly available AI tools implicates the FCA's "public disclosure bar."

Qui Tam Actions and Public Disclosure

Under the FCA *qui tam* provisions, individuals (known as "relators") can bring actions on behalf of the government. If successful, relators can receive a share of the proceeds of any award or settlement. This can be big business. In 2022, *qui tam* actions made up almost 90 percent of the government's $2.2 billion recovered under the FCA.

Authors

Nick Peterson
Of Counsel
202.719.7466
npeterson@wiley.law

Spencer C. Brooks
Associate
202.719.4571
scbrooks@wiley.law

Practice Areas

Artificial Intelligence (AI)

Civil Fraud, False Claims, *Qui Tam* and Whistleblower Actions

White Collar Defense & Government Investigations

To prevent parasitic lawsuits by opportunistic relators who convert previous disclosures of fraud into *qui tam* actions, the FCA includes what is known as the "public disclosure bar." The public disclosure bar arises as a defense to an FCA claim if the "allegations or transactions" discussed in the *qui tam* complaint have been publicly disclosed through certain channels such as the news media, government reports, government hearings, or government audits.[1] When analyzing whether such a disclosure has occurred, some courts ask whether "X + Y = Z?" Where Z represents the fraud and X and Y represent the allegations or transactions from which the fraud can be inferred. For the bar to apply, the combination of X and Y must be publicly disclosed.

If a "public disclosure" is established, a relator can still avoid dismissal if the relator demonstrates they are an "original source," which typically means they have knowledge that is *independent* of the public disclosure and that *materially adds* to publicly disclosed allegations.

The Intersection of AI and the Public Disclosure Bar

Government agencies have been using data analytics tools to prosecute fraud for years. For example, the DOJ's Health Care Fraud Unit describes itself as a "leader in using advanced data analytics and algorithmic methods to identify newly emerging health care fraud schemes and to target the most egregious fraudsters." [2] Data analytics has also been employed by the DOJ to catch Payment Protection Program (PPP) fraudsters with "unparalleled speed"[3] and to identify and prosecute insider trading.[4]

In a similar vein, the increased accessibility to large amounts of data over the Internet, coupled with the potential for significant recovery, has recently spurred the rise of relators who employ data analytics and data mining to bring FCA enforcement actions. For example, relators have used data analytics to review government data related to Medicare claims or loans under the PPP to identify potential fraudsters and bring large FCA Actions.

Given the recent surge in the availability of generative artificial intelligence and large language models, it is only a matter of time before savvy relators use AI tools to develop theories of liability, make connections across large datasets, or otherwise support *qui tam* actions. However, the use of AI tools by relators to bring FCA claims raises significant questions related to the public disclosure bar.

Most generative AI tools are themselves publicly available and are also trained on large datasets comprising, at least in part, publicly available data. Thus, the use of AI alone could implicate the FCA's public disclosure bar. Moreover, generative AI's reliance on publicly available data could pose thorny questions for litigants. Most notably, there may be challenges in identifying specific public disclosures as such tools will generally not provide references or information on specific sources. And not all publicly available data is necessarily a "public disclosure" under the FCA as the statute defines a "public disclosure" as only arising from certain enumerated sources.

Assuming a "public disclosure" is identified, a relator who relied upon AI tools to generate their allegations may find it difficult to demonstrate that they are an original source. A relator may also face challenges in proving their information is "independent" of previously identified public disclosures or explaining how allegations based on AI outputs materially add to any public disclosures.

The evolving landscape around how AI tools are trained further complicates this issue. For example, President Biden recently issued a sweeping executive order aimed at addressing AI and specifically highlighting the need to expand "public access to Federal data assets in a machine-readable format," while also ensuring the privacy of potentially sensitive training data.[5]

Impact on FCA Litigation

While it is impossible to predict with certainty how courts will grapple with these issues, there are strategies that both relators and defendants can use to best position themselves with respect to AI use and the FCA's public disclosure bar.

Relators should view AI as simply a tool: they should not rely solely on AI for FCA allegations and, instead, seek to combine it with their own evidence or insights. Relators could also try to strategically draft AI prompts to limit public disclosure concerns. Finally, the public disclosure bar allows the federal government essentially to veto the defense. Relators could advocate that the government exercise this right early on based on the potential merits of the case. This strategy would allow relators to sidestep any thorny issues related to the public disclosure bar.

Defendants should push to learn as early as possible about whether AI was used in crafting allegations—ideally while the *qui tam* complaint is under seal and the federal government is conducting its investigation. If AI was used and a public disclosure bar defense looks promising, defendants could seek to bifurcate discovery, so the initial phase of discovery focuses solely on the relator's use of AI. At the very least, defendants should use the full range of discovery tools to learn about a relator's use of AI so a public disclosure bar defense can be adequately evaluated. Finally, defendants could push the federal government to use their authority under 31 U.S.C. § 3730(c)(2)(A) to dismiss the complaint entirely. The federal government may want to curb the use of AI in *qui tam* cases to the extent such cases merely regurgitate public information.

At bottom, these are open questions that courts will likely have to grapple with sooner rather than later. Relators and defendants faced with the use of AI in an FCA action should continue to monitor developments in FCA case law and the federal regulatory landscape surrounding AI.

[1] 31 U.S.C. § 3730(e)(4)(A).

[2] https://www.justice.gov/criminal/criminal-fraud/health-care-fraud-unit

[3] https://www.justice.gov/opa/speech/acting-assistant-attorney-general-brian-rabbitt-delivers-remarks-ppp-criminal-fraud

[4] https://www.justice.gov/opa/pr/ceo-publicly-traded-health-care-company-charged-insider-trading-scheme

[5] https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/