Published on *The National Law Review* https://natlawreview.com

Cybersecurity Whistleblower Receives $499,500 in Qui Tam Settlement

Article By:

Nicolas Enrique O'Connor

On May 1, 2024, the Department of Justice ("DOJ") announced a $2.7 million dollar settlement with Insight Global LLC to resolve allegations that it violated the False Claims Act ("FCA") by failing to implement appropriate cybersecurity measures to protect confidential personal health information. The Pennsylvania Department of Health, using funds from the U.S. Centers for Disease Control, hired Insight Global to staff its COVID-19 contact tracing efforts. Terralyn Williams Seilkop, a former employee of Insight Global who worked on this contact tracing contract, filed a *qui tam* lawsuit under the FCA that brought this fraud to the attention of the DOJ, and she will receive $499,500 as part of this settlement.

The *qui tam* provisions of the FCA permit whistleblowers – known as "relators" – to file a lawsuit on behalf of the federal government alleging that an individual or a company defrauded the government, and a relator is eligible to receive between 15% and 30% of the judgement or settlement in a successful *qui tam* lawsuit. In addition to receiving an award pursuant to the DOJ's settlement of the *qui tam* action itself, the relator, who repeatedly raised concerns about this fraud and subsequently experienced being ostracized and losing job responsibilities before suffering a constructive discharge, also entered into a separate settlement agreement with Insight Global to resolve her FCA retaliation claims under 31 U.S.C. § 3730(h) for an undisclosed amount.

The DOJ alleged that, despite representing to the Pennsylvania Department of Health that it "recognizes and accepts that the contact tracing workforce will have access to personal health information of contact tracing subjects and must ensure that and all other such information related to the services being provided must be kept confidential and secure," Insight Global failed to implement cybersecurity controls and procedures. Among Insight Global's cybersecurity failures, staff hired by Insight Global shared and received personal health information and personally identifiable information through unencrypted emails and shared amongst themselves passwords to access this information. Staff also stored this information in unsecured Google Drive files that could be accessed by any member of the public through an internet link. Even though it received reports of these cybersecurity failures from its managers as early as November 2020, Insight Global failed to begin remediating these issues until April 2021.

Cybersecurity-related fraud has been a priority for the DOJ for several years. On October 6, 2021, the DOJ announced its Civil Cyber-Fraud Initiative. This initiative aims to combat fraud by companies

that knowingly provide deficient cybersecurity services, misrepresent the adequacy of their cybersecurity measures, or violate their obligations to monitor and promptly report cybersecurity events or data breaches. The DOJ has previously secured several other settlements resulting from cybersecurity-related FCA actions.

National Law Review, Volume XIV, Number 136