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

DOJ Shows its Commitment to Cybersecurity Enforcement Through the False Claims Act

Article By:

Jason Mehta

Joseph W. Swanson

At one time, False Claims Act (FCA) investigations and enforcement actions were largely focused on health care and defense contracts. While those two areas continue to dominate the FCA landscape, cybersecurity has emerged as a hot area not only for whistleblowers but also for U.S. Department of Justice (DOJ) prosecutors. Several recent developments illustrate this trend and signal that cybersecurity enforcement through the FCA will only increase.

In 2021, the DOJ launched its Civil Cyber-Fraud Initiative, which seeks to use the FCA to prosecute cybersecurity-related fraud committed by government contractors and grant recipients. Since its launch, the DOJ has announced multiple settlements under the FCA.

The following recent developments underscore the DOJ's interest in this area:

- Earlier this year, the DOJ intervened in an FCA matter initiated by two whistleblowers, which alleged that Georgia Tech Research Corporation and the Georgia Institute of Technology (Georgia Tech) violated various cybersecurity requirements that are part of Department of Defense contracts.
- In May 2024, the DOJ announced a US$2.7 million settlement with Insight Global LLC. The matter involved whistleblower allegations that the company failed to implement sufficient cybersecurity measures to protect health information collected as part of COVID-19 contact tracing. These failures allegedly violated the FCA and included allegations that the company had not responded in a timely manner to concerns raised internally regarding the security failures. Notably, the contract at issue was a state contract that used federal funds.
- In June 2024, DOJ announced an US$11.3 million settlement with two consulting companies that allegedly violated the FCA by failing to comply with cybersecurity requirements as part of a federally-funded state contract to facilitate applications for federal rental assistance. This matter also began with a whistleblower complaint.

Given the emergence of cybersecurity as an area of focus within the FCA, organizations should focus on the following action items to enhance cybersecurity compliance and reduce FCA risk:

1. **Catalogue and monitor compliance with all government-imposed cybersecurity standards**. This includes not only ongoing knowledge of the organization's contracts, but also continuously monitoring and assessing the organization's cybersecurity program to identify and patch vulnerabilities and to assess compliance with those contractual cybersecurity standards.
2. **Developing and maintaining a robust and effective compliance program**. In such a program, employees are encouraged to report concerns, and those concerns are investigated promptly and escalated as appropriate.
3. **Where non-compliance with cybersecurity standards is identified, organizations should evaluate potential next steps**. This includes whether to disclose the matter to the government and cooperate with government investigators. Organizations should work with experienced counsel in this regard. Proactively mapping out a strategy for investigating and responding to potential non-compliance can instill discipline to the process and streamline the organization's approach.

National Law Review, Volume XIV, Number 219