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

Latest Cyber-Related FCA Settlement Underscores the Breadth of DOJ's Civil Cyber-Fraud Focus

Article By:

Townsend L. Bourne

Nikole Snyder

On June 17, 2024, the Department of Justice ("DOJ") announced the latest settlement under its Civil Cyber-Fraud Initiative ("CCFI") (previously discussed here).[1] The settlement resulted in a total of $11,300,000 in payments from two consulting companies (Guidehouse, Inc., the prime contractor, which paid $7,600,000; and Nan Kay and Associates, the subcontractor, which paid $3,700,000) to resolve allegations the two companies violated the False Claims Act by failing to meet cybersecurity requirements in federally-funded contracts.

Guidehouse entered into a contract in 2021 with the New York Office of Temporary Disability Assistance ("OTDA") to assume responsibility over the emergency rental assistance program ("ERAP") in New York, which included managing the application platform for distribution of federal funding to eligible low-income households to cover certain costs during the COVID-19 pandemic. Under the respective contracts, both Guidehouse and its subcontractor, Nan Kay and Associates, were responsible for ensuring the application platform underwent cybersecurity testing before it was provided to the public. However, neither company satisfied that obligation, and 12 hours after the website went live, OTDA shut it down because certain applicants' personally identifiable information ("PII") was compromised and generally available on the internet. Additionally, for a short time in 2021, Guidehouse admitted it used a third-party data cloud software program to store PII, without first obtaining permission from OTDA, in violation of its contract.

This settlement is notable because it continues to underscore the breadth of the CCFI's ambit. Here are three key reminders about CCFI enforcement:

- It is not limited to federal contracts. As we saw with the earlier Jelly Bean settlement, the contractual obligations here stem from a *state* government contract, rather than a federal contract. Yet, the misconduct still falls under DOJ's purview because the contract was funded with federal dollars. Accordingly, contractors who enter into contracts with *any* government entity should pay close attention to the contract language, funding source, and contractual requirements.
- It is not limited to prime contractors. This settlement involved not only the prime contractor (Guidehouse), but also its subcontractor (Nan Kay). This is a good reminder that the False

Claims Act is not limited to the contractor with the direct contractual relationship with the government. It also reaches subcontractors (or lower-tier contractors) that cause the prime contractor to make a false claim for payment.
- It is not limited to a particular industry. We have seen settlements and complaints against companies in a range of industries, including health services, aerospace & defense, data hosting, communications, higher education and associated research centers, staffing services, and technology consulting. This emphasizes that anyone doing business with the government should be mindful of their cybersecurity obligations.

The number and cadence of CCFI settlements and complaints demonstrates that enforcing cybersecurity obligations remains a top priority for DOJ. As such, companies doing business with the government—in all industries and at all levels of the supply chain—must ensure they understand and comply with applicable cybersecurity requirements.

FOOTNOTES

[1] Since the inception of the CCFI in October 2021, the DOJ has announced six cyber-fraud related settlements, totaling approximately $28.2 million. There also are at least two ongoing *qui tam* cases that have not yet reached a resolution.

Listen to this post

National Law Review, Volume XIV, Number 179