Buchalter

CLIENT ALERT

March 28, 2023

Taste-Testing Cybersecurity Compliance: A Recipe for Disaster in Government Contracting

By: Meghna Parikh

The Department of Justice (DOJ) Civil Cyber-Fraud Initiative continues to raise the stakes for government contractors. This initiative uses the False Claims Act ("FCA") to hold government contractors accountable for knowingly (1) failing to monitor and report cyber data breaches, (2) implementing inadequate cybersecurity measures or (3) misrepresenting their cybersecurity practices. According to a DOJ press release, website design provider Jelly Bean Communications ("Jelly Bean") is the latest in their roster of settled false claims from cybersecurity non-compliance. From 2014 until 2020, Jelly Bean created, hosted, and maintained the website HealthyKids.org for Florida Healthy Kids Corporation, including the online application into which parents and others entered data to apply for state Medicaid insurance coverage for children. In December 2020, over half a million applications submitted on HealthyKids.org were revealed to have been hacked, potentially exposing the applicants' personal identifying information and other data. Jelly Bean included a line item on invoices for "HIPAA-compliant hosting," while knowingly failing to properly maintain, patch, and update software systems.

Part of the DOJ's reasoning in applying the FCA to these three new categories is that an organization's failure to adequately protect patient information deprives the government of what it bargained for, which is deemed a false claim. Because most healthcare organizations qualify as government contractors by way of participating in Medicare/Medicaid, this extension of the FCA to cybersecurity practices could put the majority of them at much greater risk of running afoul of the FCA.

This recent settlement with Jelly Bean highlights the need for secure hosting of personal information, maintenance of software systems, and compliance with cybersecurity standards in addition to protective contractual language. The DOJ's eagerness to hold government contractors accountable for contractual breaches under FCA demonstrates the importance of complying with evolving cybersecurity requirements and being able to demonstrate this compliance in the fact of an audit. To protect against these risks, government contractors should be careful about delegating cybersecurity compliance, including by working with experienced legal counsel, to ensure compliance with evolving cybersecurity requirements. If you have any questions, please contact the author or your Buchalter relationship attorney.

Meghna Parikh
Attorney
(213) 891-5264
mparikh@buchalter.com