Proskauer

Another Resolution by DOJ Pursuant to its Civil Cyber-Fraud Initiative Highlights Continued Efforts to Hold Companies Accountable for Ensuring Data are Secured

Health Care Law Brief on **June 5, 2023**

We previously wrote about the United States Department of Justice's ("DOJ") Civil Cyber-Fraud Initiative ("CCFI"), which "aims to hold accountable entities or individuals that put U.S. information or systems at risk by knowingly providing deficient cybersecurity products or services, knowingly misrepresenting their cybersecurity practices or protocols, or knowingly violating obligations to monitor and report cybersecurity incidents and breaches." In that post, we summarized DOJ's first two False Claims Act ("FCA") resolutions pursuant to the CCFI, which amounted to more than $9 million in recoveries.

As part of its continued efforts to "combat new and emerging cyber threats to the security of sensitive information and critical systems," DOJ announced another resolution. Specifically, DOJ entered into an FCA settlement agreement with Jelly Bean Communications Design LLC ("Jelly Bean") and its manager, Jeremy Spinks ("Spinks"), to resolve allegations that they failed to secure personal information on a federally-funded Florida children's health insurance website called HealthyKids.org, which was created, hosted, and maintained by Jelly Bean. To resolve these allegations, Jelly Bean and Spinks agreed to pay $293,771.

In 2013, Jelly Bean contracted with the Florida Health Kids Corporation ("FHKC")—a state-created entity that offers health and dental insurance for Florida children—to create, host, and maintain HealthyKids.org, where, in part, parents and others could apply for state Medicaid insurance coverage for eligible children. Under its agreement with FHKC, Jelly Bean was required to provide a fully-functional hosting environment that complied with HIPAA rules, including ensuring the security of protected health information ("PHI") entered and maintained on the website for purposes of a parents' or others' application for state Medicaid insurance coverage for eligible children.

The FCA settlement agreement alleged that, for about seven years, Jelly Bean did not provide secure hosting of the applicants' PHI, but instead knowingly failed to properly maintain, patch, and update software systems underlying HealthyKids.org and related websites. Jelly Bean's failure left the website and such PHI vulnerable from attack. Despite not providing the foregoing, Jelly Bean represented compliance with its contract with FHKC. In or around December 2020, more than half a million applications submitted on HealthKids.org were hacked and the PHI contained therein were potentially exposed. DOJ determined that, at that time, Jelly Bean was running multiple outdated and vulnerable applications, including software that had not been updated since only a month after entering into its contract with FHKC—in 2013. FHKC shut down its website's application portal shortly thereafter.

Government contractors, such as Jelly Bean, are expected "to do the due diligence to keep software applications updated and secure" to ensure the "safeguarding [of] patients' medical and other personal information." Just as it was emphasized by DOJ when it announced the CCFI and its first two FCA resolutions pursuant to the CCFI, the government re-emphasized that it "will continue to work … to ensure that enrollees can rely on their health care providers to safeguard their personal information."

View original.

Related Professionals

- **Matthew J. Westbrook**
  Senior Counsel