BARNES & THORNBURG LLP

ALERTS

HIPAA Data Breach Costs Company Nearly $300,000 In DOJ False Claims Act Settlement

April 4, 2023

Highlights

HIPAA business associates that have government contracts can face FCA penalties in addition to sanctions under HIPAA

A web-hosting company paid $293,771 to settle FCA allegations that it failed to secure personal information

This settlement is confirmation that the DOJ will continue using the FCA to address HIPAA violations and substandard cybersecurity practices

On March 14, 2023, the U.S. Department of Justice (DOJ) announced the settlement of a case involving alleged violations of the False Claims Act (FCA) as a result of cybersecurity failures and breach of HIPAA-protected health information. Obtained under the Civil Cyber-Fraud Initiative, this settlement emphasizes that HIPAA business associates that have government contracts can face FCA penalties from federal law enforcement in addition to the monetary penalties pursued by the Office for Civil Rights, which enforces HIPAA.

Under the settlement agreement, Jelly Bean Communications Design LLC agreed to pay $293,771 to resolve FCA allegations that it failed to secure

RELATED PEOPLE

Stacy L. Cook
Partner
Indianapolis

P 317-231-7237
F 317-231-7433
stacy.cook@btlaw.com

Iqra Mushtaq
Associate
Chicago

P 312-214-5614
F 312-759-5646
iqra.mushtaq@btlaw.com

RELATED PRACTICE AREAS

Compliance and Monitorships
Data Security and Privacy

RELATED INDUSTRIES

Healthcare

personal information on the Florida Healthy Kids Corporation (FHKC) website, which Jelly Bean created, hosted and maintained. FHKC contracts with the state of Florida to provide services for the State Children's Health Insurance Program. The federal government funded 86 percent of the payments made from FHKC to Jelly Bean.

According to the settlement agreement, in early December 2020 it became apparent that more than 500,000 applications submitted on the website had been hacked by third parties. An independent investigation by FHKC revealed that the hackers altered applications and the website was running multiple outdated and vulnerable applications. The settlement agreement alleges Jelly Bean did not maintain adequate audit logs showing who accessed applicants' personal information, but the information potentially exposed by the website's vulnerabilities included very sensitive information about applicants, including full name and date of birth; email address and telephone number; physical and mailing address; and Social Security number.

The Civil Cyber-Fraud Initiative, established in October 2021, is led by the DOJ's Civil Fraud Section and focuses on using the FCA to hold accountable entities or individuals that put U.S. information or systems at risk by knowingly failing to comply with required cybersecurity standards, misrepresenting cybersecurity controls and practices, failing to monitor cybersecurity systems, and failing to timely report cyber incidents and breaches. The DOJ announced its first settlement under the initiative on March 8, 2022.

This settlement is confirmation that the DOJ intends to continue using the FCA to address HIPAA violations and substandard cybersecurity practices.

For more information, please contact the Barnes & Thornburg attorney with whom you work or Stacy L. Cook at 317-231-7237 or stacy.cook@btlaw.com or Iqra Mushtaq at 312-214-5614 or iqra.mushtaq@btlaw.com.