MINTZ

EnforceMintz — 2023 Brings Uptick in Cybersecurity Enforcement, Insight Into Potential Risks

February 08, 2024 | Blog | By **Samantha P. Kingsbury**

VIEWPOINT TOPICS

- Health Care Enforcement & Investigations
- Health Care

RELATED PRACTICES

- Health Care Enforcement & Investigations

RELATED INDUSTRIES

- Health Care

After the **Department of Justice ("DOJ") announced its Civil Cyber-Fraud Initiative in October 2021**, many in the False Claims Act ("FCA") bar expected an onslaught of enforcement actions and *qui tam* cases. The initiative started off slow in 2022, with the government announcing only two cybersecurity-related settlements (we covered **one of those settlements** in our February 2023 edition of *EnforceMintz*, and you can find more information about the second settlement **here**). But in 2023 we started to see an uptick in activity: two cybersecurity-related FCA settlements, an unsealed *qui tam* complaint, and significant regulatory activity that could pose future enforcement risk. While the developments in this space may seem relatively limited, they emphasize the breadth of potential entities, types of conduct or missteps, and legal requirements that may be subject to enforcement under DOJ's Civil Cyber-Fraud Initiative or other applicable authorities.

Jelly Bean Communications Design

In March, **DOJ announced** that Jelly Bean Communications Design and its manager had agreed to pay approximately $294,000 to **resolve FCA allegations** that they failed to secure personal information on a website that Jelly Bean had created, hosted, and maintained for the Florida Healthy Kids Corporation ("FHKC"). FHKC received state and federal Medicaid funds to offer health and dental insurance coverage for Florida. Jelly Bean had agreed to provide a HIPAA-compliant hosting environment, but instead it knowingly failed to maintain, patch, and update the necessary software systems, which left the relevant websites vulnerable to cyberattacks.

In December 2020, more than 500,000 applications submitted on one of the websites Jelly Bean operated for FHKC were hacked, exposing the applicants' personal identifying information. DOJ thus alleged that Jelly Bean submitted, or caused to be submitted, false claims for federal funds paid through the contracts that Jelly Bean had with FHKC and that FHKC had with the Florida Agency for Health Care Administration, the Florida agency that had contracted with FHKC to provide services for the State Children's Health Insurance Plan Program.

Verizon Business Network Services

In September, **DOJ announced** that Verizon Business Network Services ("Verizon") had agreed to pay approximately $4 million to resolve allegations that it had violated the FCA by failing to fully satisfy three cybersecurity controls in connection with its Managed Trusted Internet Protocol Service ("MTIPS"), which is supposed to provide to federal agencies a secure connection to the public internet and external networks in compliance with the **Office of Management and Budget's Trusted Internet Connections** ("TIC") initiative. These cybersecurity requirements related to contracts Verizon had with the General Services Administration from 2017 to 2021, which required compliance with all Critical Capabilities specified in the Department of Homeland Security's TIC Reference Architecture Document.

Another notable feature of this resolution is that both the **DOJ press release** announcing the settlement and **the settlement agreement** itself detail how Verizon took significant steps that resulted in the company obtaining **cooperation credit** from the government.

Penn State University

Also in September, the US District Court for Eastern District of Pennsylvania unsealed the complaint in ***United States ex rel. Decker v. Pennsylvania State University*, 22-cv-03895-PD**. In this case, Matthew Decker, the Chief Information Officer ("CIO") for Penn State's Applied Research Laboratory and former

interim CIO for the university itself, is the relator. In short, Mr. Decker alleges that Penn State violated the FCA by submitting to the Department of Defense ("DoD") false attestations of compliance with cybersecurity standards applicable to federal contractors that possess controlled unclassified information, among other violations.

All three of these matters (Jelly Bean, Verizon, and Penn State) demonstrate the wide range of entities that may be susceptible to FCA liability for potential cybersecurity failures. They likewise emphasize the wide range of services — website hosting, secured internet connectivity, and applied research — and sources of cybersecurity-related requirements (contracts, agency-issued requirements, regulations), that may serve as the basis for FCA allegations.

Cybersecurity-Related Regulatory Developments

In 2023, two agencies released final and proposed rules that might add to existing avenues of potential legal exposure for cybersecurity-related noncompliance, including for publicly traded health care companies and health care providers and companies that provide items or services to the federal government through federal contracts subject to the Federal Acquisition Regulation ("FAR").

In September, the Securities and Exchange Commission ("SEC") **adopted rules on disclosures regarding cybersecurity risk management**. These rules "enhance and standardize disclosures regarding cybersecurity risk management, strategy, governance, and incidents by public companies subject to the reporting requirements of the Securities Exchange Act of 1934."Notable features of the SEC rules include (1) amendments to require current disclosure of material cybersecurity incidents, and (2) requirements around periodic disclosure about a registrant's process to assess, identify, and manage cybersecurity risk, as well as the roles played by management and the board of directors in those areas.

In October, the FAR Council proposed rules that would increase cybersecurity requirements applicable to federal contractors. More specifically, **the first FAR rule** proposes to standardize contractual requirements related to cybersecurity across all federal agencies. The **second FAR rule** proposes to amend the Federal Acquisition Regulation to require increased information-sharing and disclosure around cyber threats and incidents. For example, if made law, this rule would require federal contractors to report security incidents *within eight hours of discovery*, among a variety of other requirements.

This expansion of legal requirements — alongside the rapid evolution of how federal contractors and other entities use or offer services related to electronic data and technology — will almost certainly continue to expand the types of enforcement action we see in this space. These developments likewise serve as an important reminder that health care providers and companies should be familiar with applicable cybersecurity-related requirements and ensure that they have a process in place to verify compliance with those requirements, especially before certifying compliance to the government.

Authors

Samantha P. Kingsbury, Of Counsel

Samantha advises clients on regulatory and enforcement matters. She has deep experience handling violations of the federal ant-kickback statute and FCA investigations for clinical laboratories and hospitals.