The FTC's Retooled Data Security Orders

Friday, May 10, 2019

JB Kelly spoke with *FTC Watch* about the FTC's April 24, 2019, settlement orders in cases against ClixSense and i-Dressup. After the 11th Circuit ruled in June 2018 that an FTC order telling LabMD to "fix its weak data security" was too vague to be enforceable, the FTC issued orders last month providing a bit more detail about its expectations regarding a company's data security efforts.

The FTC's April 24, 2019, settlement orders in cases against ClixSense and i-Dressup could potentially serve as "a blueprint of what they are going to be asking everybody to do," said JB Kelly, who handled the matter for ClixSense and its founder. The FTC's April 2019 orders outline certain elements, including: implementing comprehensive information security programs, obtaining independent biennial assessments, and obliging a senior officer to provide the FTC with annual compliance certifications.

As Kelly pointed out, the FTC said [the company] "'must, at a minimum' take eight detailed steps — A through H — to show it's maintaining a comprehensive information security program." However, "the words 'at a minimum' give the agency the ability to subsequently define the elements necessary to have a comprehensive information security program — not define it up front," he said.

The FTC's Robert Schoshinski stated that their goal is "not to be overly prescriptive." But Kelly noted "they are not quite willing to narrowly, specifically define actions that people have to take." Vague requirements prompted the appellate court in LabMD to throw out the agency's order. So, Kelly said, "there are still risks for the FTC" in mandating what it calls "a comprehensive information security program."

To read more of the article, **click here.** *(Subscription required)*

Related Practice Areas

- State Attorneys General

COZEN O'CONNOR