FTC settles with Schein for false advertising of encryption

False advertising of HIPAA-standard encryption

On 5 January 2016, the Federal Trade Commission (‘FTC’) announced that Henry Schein Practice Solutions, Inc. (‘Schein’) would pay $250,000 dollars to settle the FTC’s charge for falsely advertising that Schein’s Dentrix G5 software enabled dentists to meet the Health Insurance Portability and Accountability Act 1996 (‘HIPAA’) encryption requirements.

The Office for Civil Rights’ (‘OCR’) guidance on encryption standards provides covered entities with resources from the National Institute of Standards and Technology (‘NIST’), which list encryption algorithms that meet the regulatory obligations of HIPAA’s encryption standard (45 C.F.R. 164.304). In early 2012, Schein introduced Dentrix G5, a practice management software for dentists. Schein purported that the software allowed dental providers to collect and store patient information safely and securely due to its “new encryption capabilities.” Other marketing also claimed that the information was stored in an “encrypted format” and would protect users from hackers. Schein marketed Dentrix G5 to dental practices throughout the US. In November 2010, the third-party vendor who created the database engine that was incorporated in Dentrix G5 informed Schein that the software did not use any NIST standards for its encryption, but instead used a proprietary algorithm that had not been tested publicly, and was less secure and more vulnerable than other available algorithms.

Despite having knowledge that its product did not provide the level of encryption security required by HIPAA, Schein advertised Dentrix G5 as a product that would provide the encryption necessary for covered entities to meet HIPAA requirements. In early June 2013, the US Computer Emergency Readiness Team (‘US-CERT’) issued a vulnerability note regarding the data protection used by Dentrix G5, and NIST posted a corresponding vulnerability alert in late June 2013. Schein’s third party database vendor agreed to re-brand the algorithm in the Dentrix G5 as ‘Data Camouflage’ so that it would not be mistaken for actual encryption. Schein did not change its advertising for Dentrix, continuing to claim that Dentrix G5 provided encryption and did not update consumers who were using Dentrix G5 and advise them that the software was not sufficient for HIPAA compliance for collection and storage of protected health information. Schein continued to sell this product even after these alerts were issued.

The FTC order requires Schein to pay a fine, identify all affected customers who purchased the software prior to January 2014 and mail all customers a notice with information about standards and Dentrix G5’s failure to meet those standards, along with a toll-free number and email address for inquiries.

Who is ready for the FTC?

Section 5 of the FTC Act prohibits ‘unfair or deceptive acts or practices in or affecting commerce.’ 15 U.S.C. §45(a)(1). The FTC has on at least four separate occasions pursued HIPAA-

covered entities or business associates for representing that data was securely transmitted or stored when in fact, data was either indexed online, inadequately safeguarded on devices, or improperly disposed. The Schein consent agreement signals that the FTC will continue an aggressive course in regulating and enforcing data privacy and security, whether the FTC investigates in conjuction with the OCR or independently.

Mitigating harms and preparing for scrutiny

The FTC has analysed all of its consent agreements and prepared ‘Start with Security: A Guide for Business,’ which contains ten areas of focus for businesses’ data privacy and security practices, including: (1) start with security; (2) control access to data sensibly; (3) require secure passwords and authentication; (4) store sensitive personal information securely and protect it during transmission; (5) segment your network and monitor who's trying to get in and out; (6) secure remote access to your network; (7) apply sound security practices when developing new products; (8) make sure your service providers implement reasonable security measures; (9) put procedures in place to keep your security current and address vulnerabilities that may arise; and (10) secure paper, physical media, and devices. This guidance is the most thorough data privacy and security guidance provided by the FTC to date.

Since the FTC uses Section 5 in its enforcement, a pattern is developing in these data privacy and security investigations. The entities that the FTC investigates do not ensure that their message to consumers or customers is consistent with the actual services being provided. The FTC considers this to be unfair deceptive trade practices and moves forward with enforcement; the Schein consent agreement demonstrates this. Schein could have mitigated the FTC findings had it promptly addressed the gap between encryption that its software provided and what it claimed to customers and potential customers.

Healthcare organisations and their business partners can protect themselves from both loss of data and regulatory scrutiny and enforcement by addressing risk vulnerabilities and keeping documentation of the same. Healthcare organisations face increased regulatory scrutiny for the protection of patient information and should confirm that they are meeting the minimum requirements under HIPAA as well as ensuring that any public-facing communications are current and truthful as to the protection of that information. These recent regulatory actions demonstrate that both the FTC and the OCR focus on the healthcare entity’s analysis of risks and risk management of the same in reaching their conclusions.

Lynn Sessions Partner
Suchismita Pahi Associate
Baker Hostetler, Houston
lsessions@bakerlaw.com
spahi@bakerlaw.com