February 5, 2016

FTC's Proposed Settlement with Dental Practice Software Provider Marks Latest Data Security Action Against a Product Supplier

Attorneys
Heather Egan Sussman
Douglas H. Meal
James S. DeGraw
Seth C. Harrington
David McIntosh
Mark P. Szpak
Michelle Visser
Paul D. Rubin
Deborah Gersh
Timothy M. McCrystal
Laura G. Hoey
Marc P. Berger
David T. Cohen

On January 5, the Federal Trade Commission ("FTC") reached an agreement with Henry Schein Practice Solutions, Inc. ("HSPS") to settle allegations that HSPS misrepresented that its dental practice software provided industry-standard encryption for personal information and helped dentists meet certain regulatory data security obligations. The proposed settlement, which is now subject to a 30-day public comment period, would require HSPS to pay $250,000 and prohibit the company from misrepresenting the security features of its software. By agreeing to the proposed settlement, HSPS has not admitted to any allegations contained in the FTC's complaint. The FTC's action against HSPS reflects the agency's continued interest in the security of health information, as well as its growing focus on pursuing product manufacturers and software providers that allegedly expose personal information to a risk of unauthorized access. It also demonstrates the FTC's apparent view that a software vendor can be held liable for allegedly making deceptive statements about data security to its businesses customers, even if the statements are not made to the individuals whose personal information is allegedly put at risk of unauthorized access.

According to the FTC, HSPS sold software branded as "Dentrix G5" to dental practices, enabling dentists to perform common office tasks such as entering patient data, sending appointment reminders, processing patient payments, submitting patient insurance claims, documenting treatment planning, entering progress notes, and recording diagnostic information. The FTC alleges that dentists used this Dentrix G5 software to collect and store patients' personal information. The FTC's complaint contends that, for two years, HSPS's advertisements for Dentrix G5 represented that the software provided industry-standard encryption for this personal information and that it helped dentists meet regulatory data security obligations related to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA").

The complaint alleges that these advertisements were false or misleading. Specifically, the FTC alleges that HSPS had been informed by the vendor of the database engine for Dentrix G5 that the form of data protection it used was a proprietary algorithm that had not been tested publicly, and was less secure and more vulnerable than widely used, industry standard encryption algorithms such as Advanced Encryption Standard ("AES") encryption. The FTC also alleges that, prior to releasing Dentrix G5, HSPS was aware that the Department of Health and Human Services ("HHS") directs healthcare providers, including most dentists, to guidance promulgated by the National Institute of Standards and Technology ("NIST") to help them meet their regulatory obligations to protect patient data. The NIST guidance, the FTC alleges, recommends AES encryption. The FTC also contends that HSPS was aware that HHS' Breach Notification Rule requires dentists to notify patients of certain breaches, but includes a "safe harbor" so that dentists would not have to notify patients about breached data that was encrypted consistent with NIST Special Publication 800-111.

The complaint further alleges that, in June 2013, the United States Computer Emergency Readiness Team ("US-CERT") issued a Vulnerability Note describing the form of data protection used in Dentrix G5 software as a "weak obfuscation algorithm," and that NIST published a corresponding vulnerability alert the same month. According to

the FTC, the US-CERT Vulnerability Note stated that the database engine vendor had agreed to rebrand the data protection as "Data Camouflage" so it would not be confused with standard encryption algorithms, such as AES encryption. The FTC contends that, despite receiving notice of the US-CERT Vulnerability Note and the database vendor's decision to rebrand in June 2013, HSPS continued for an additional seven months to disseminate marketing materials stating that Dentrix G5 "encrypts" patient data and offers "encryption."

The proposed consent order would prohibit HSPS, in connection with advertising a product or service designed to collect or store personal information, from misrepresenting (1) whether or to what extent the product or service offers industry-standard encryption, (2) the ability of the product or service to help customers meet regulatory obligations related to privacy or security, or (3) the extent to which a product or service maintains the privacy, security, confidentiality, and integrity of personal information. The proposed consent order would also require that HSPS notify customers who purchased Dentrix G5 that the software uses a less complex encryption algorithm to protect patient data than AES.

The proposed consent order also would require HSPS to make a monetary payment of $250,000. Under the terms of the proposed order, the payment may be deposited into a fund administered by the Commission for consumer redress. If the Commission decides that direct redress to affected dental practice customers is wholly or partially impracticable or money remains after redress is completed, the Commission may apply the remaining money for other relief (such as consumer information remedies). Any money not used is to be deposited to the U.S. Treasury. The proposed order specifies that the payment is not a fine, penalty or punitive assessment.

The proposed HSPS settlement continues the recent trend by plaintiffs and regulatory agencies to expand the pool of defendants in data security litigation. While traditionally the FTC and other public and private actors have sought to hold liable companies that collect or use personal information that is the subject of an alleged breach, they have recently sought to expand the boundaries of liability to any party who allegedly may have had some role in putting personal information at risk of unauthorized access. The FTC has been one of the primary forces behind this trend, with enforcement actions against TRENDnet, Inc. (manufacturer of web-based cameras), Upromise, Inc. (developer of a web-browser toolbar), and a recent action against Oracle (developer of a computing platform), among others, illustrating the FTC's shift in focus toward product manufacturers and software providers that allegedly expose personal information to a risk of unauthorized access. *See In re TRENDnet, Inc.*, Complaint, FTC Dkt. No. C-4426 (Jan. 16, 2014); *In re Upromise, Inc.*, Complaint, FTC Dkt. No. C-4351 (Mar. 27, 2012); *In re Oracle Corporation*, Complaint, FTC File No. 132 3115 (Dec. 21, 2015). Importantly, the HSPS matter demonstrates the FTC's apparent view that a software vendor can be held liable for allegedly making deceptive statements about data security to its businesses customers (here, the dental practices), even if the statements are not made to the individuals whose personal information is allegedly put at risk of unauthorized access.

Companies should also note the FTC's position as to what constitutes encryption, and its reliance on NIST guidance and a US-CERT Vulnerability Note as alleged support for its contention. Finally, healthcare companies in particular should note the FTC's continued interest in the security of health information, with the HSPS action coming on the heels of recent data security actions against a medical transcription provider and a medical testing laboratory. *See In re GMR Transcription Svs., Inc.*, Complaint, FTC Dkt. No. C-4482 (Jan. 31, 2014); *In re LabMD*, Complaint, FTC Dkt. No. 9357 (Aug. 28, 2013) (decision rendered against Commission; appeal pending).

* * * * *

For more information regarding the settlement between the FTC and HSPS or to discuss data security practices generally, please feel free to contact Heather Egan Sussman, Doug Meal, Jim DeGraw, Seth Harrington, David McIntosh, Mark Szpak, Michelle Visser, Paul Rubin, Debbie Gersh, Tim McCrystal, Laura Hoey, Marc Berger, David Cohen, or another member of Ropes & Gray's leading privacy & data security team.