WILMERHALE

FTC Settles with Software Provider over Encryption Claims—Order Requires $250,000 Disgorgement and Notification to Customers

JANUARY 11, 2016

On January 5, 2016, the Federal Trade Commission (FTC or "Commission") settled charges against Henry Schein Practice Solutions, Inc. ("Schein") for alleged misrepresentations regarding the level of encryption provided by the company's dental office management software. In a first for marketing claims related to data security, the proposed consent order requires the company to pay $250,000 to the FTC, as well as to notify customers of the software's lack of encryption capabilities.

The FTC's settlement offers important lessons—both for businesses and their third-party service providers—on the implications of making and evaluating representations about data security.

Misrepresentations Regarding Encryption. The complaint itself is a straightforward application of Section 5 of the FTC Act, which prohibits unfair or deceptive acts or practices. The complaint alleges that Schein advertised its office management software as having "encryption" capabilities that could help dentists meet their obligations related to the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

Despite these claims, Schein's software apparently integrated another third-party vendor's "database engine" that provided a less secure form of data protection. According to the complaint, the vendor had even informed Schein as early as 2010 that "the form of data protection...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 alleged that the software did not satisfy encryption standards for purposes of HIPAA, since HHS directs healthcare providers to follow the National Institute of Standards and Technology's (NIST) recommendations to use AES encryption.

In other words, Schein's software allegedly did not use *industry-standard* encryption technology that was capable of helping dentists protect patient data, as required by HIPAA. Therefore, the FTC alleged that Schein's representations were false and misleading, in violation of Section 5 of the FTC Act.

Failure to Heed Warnings from Third Parties. Moreover, in what has become a common refrain in

FTC data security cases, the FTC also noted that the company failed to address warnings from third parties regarding the software's lack of encryption capabilities. For example, in addition to the third-party vendor's warnings in 2010, the U.S. Computer Emergency Readiness Team issued a Vulnerability Note in 2013 that described the software's data protection features as a "weak obfuscation algorithm." Shortly thereafter, NIST published a corresponding vulnerability alert. Notwithstanding those warnings, Schein allegedly continued to disseminate marketing materials that described its software as having "encryption" capabilities.

Role as a Third-Party Service Provider. The FTC's complaint emphasizes Schein's role as a third-party service provider and its impact on dentists' ability to protect patient data as required by HIPAA. For example, the complaint noted that dentists used the software to collect and store patients' sensitive personal information, including Social Security Number, driver's license number, web user ID and password, clinical notes, prescriptions, and diagnoses. As a result, the FTC alleged that, absent Schein's misrepresentations, its customers might have made different purchasing decisions or taken other steps to protect patients' sensitive personal information. The FTC also noted that in cases where a breach might occur, dentists "may mistakenly believe they qualify for the encryption safe harbor under the Breach Notification Rule, and are not required to notify patients in the event of a breach" or, alternatively, "may misinform patients about their risk of identity theft by telling them that the lost data was 'encrypted.'"

In other words, the FTC believed that the misrepresentations would influence dentists' purchase and use of the software, and their compliance obligations with respect to HIPAA, and thus were material under Section 5.

$250,000 Disgorgement, Customer Notification, and Other Requirements.The proposed consent order is notable for the breadth of remedies sought by the Commission. For example, the consent order requires that Schein pay $250,000 in disgorgement to the FTC, which an FTC blog post notes is "a fairly common provision in FTC advertising cases, *but a first for marketing claims specifically related to data security*." (emphasis added). The 20-year consent order also requires Schein to notify customers that the software "uses a less complex encryption algorithm to protect patient data than [AES], which is recommended as an industry standard by [NIST]." It also prohibits Schein from making future misrepresentations and requires Schein to comply with reporting, recordkeeping, and other administrative requirements.

Implications for Businesses and Their Service Providers. The FTC's complaint offers important lessons—both for businesses and their third-party service providers—on the implications of making and evaluating representations about data security:

- ***First***, companies should be very careful when making express claims about specific data security measures, such as encryption. If a company does make an express claim regarding data security, it should ensure that it is accurate and not misleading;
- ***Second***, service providers should ensure that all statements related to data security, including marketing claims to their business customers, are accurate and not misleading;
- ***Third***, companies should consider implementing a process to receive and address security warnings from third parties, as recommended by the FTC's Start with Security

guidance; and

- ***Fourth***, businesses should take steps to verify third-party vendors' security claims, to the extent possible, especially if those claims impact a company's compliance with specific laws. As we have described in an earlier article, vendor oversight is an important part of complying with the FTC's expectations on privacy and security.

Wilmer Cutler Pickering Hale and Dorr LLP is a Delaware limited liability partnership. WilmerHale principal law offices: 60 State Street, Boston, Massachusetts 02109, +1 617 526 6000; 2100 Pennsylvania Avenue, NW, Washington, DC 20037, +1 202 663 6000. Our United Kingdom office is operated under a separate Delaware limited liability partnership of solicitors and registered foreign lawyers authorized and regulated by the Solicitors Regulation Authority (SRA No. 287488). Our professional rules can be found at www.sra.org.uk/solicitors/code-of-conduct.page. A list of partners and their professional qualifications is available for inspection at our UK office. In Beijing, we are registered to operate as a Foreign Law Firm Representative Office. This material is for general informational purposes only and does not represent our advice as to any particular set of facts; nor does it represent any undertaking to keep recipients advised of all legal developments. Prior results do not guarantee a similar outcome. © 2004-2024 Wilmer Cutler Pickering Hale and Dorr LLP