1423161

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

COMMISSIONERS: **Edith Ramirez, Chairwoman**
Maureen K. Ohlhausen
Terrell McSweeny

In the Matter of **HENRY SCHEIN** **PRACTICE SOLUTIONS, INC.,** **a corporation.**	**DOCKET NO. C-4575**

COMPLAINT

The Federal Trade Commission, having reason to believe that Henry Schein Practice Solutions, Inc., a corporation, has violated the provisions of the Federal Trade Commission Act, and it appearing to the Commission that this proceeding is in the public interest, alleges:

1. Respondent Henry Schein Practice Solutions, Inc. ("Henry Schein") is a Utah corporation with its principal office or place of business at 1220 South 630 East, American Fork, Utah 84003.

2. Respondent manufactures, advertises, offers for sale, sells, and distributes office management software for dental practices, including but not limited to the Dentrix software described below.

3. The acts or practices of Respondent alleged in this complaint have been in or affecting commerce, as "commerce" is defined in Section 4 of the Federal Trade Commission Act.

Respondent's Business Practices

4. Dentrix software enables 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.

5. In the spring of 2012, Respondent introduced the Dentrix G5 software ("Dentrix G5"). Dentrix G5 incorporated a new "database engine" provided by a third-party vendor, which

included new capabilities, including a form of data protection that Respondent advertised as "encryption."

6. Dentists use Dentrix G5 to collect and store patients' personal information. The personal information can consist of sensitive information about patients, including, in some instances:

> name, address, telephone number, Social Security number, date of birth, driver's license number, email address, web user ID and password, picture, name of insurance providers, clinical notes, prescriptions, and diagnoses.

7. As early as November 2010, the database engine vendor informed Respondent that the form of data protection used in Dentrix G5 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.

8. Prior to releasing Dentrix G5, Respondent 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 recommends AES encryption. Respondent was also aware that HHS' Breach Notification Rule, 45 C.F.R. §§ 164.400-414, 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.

9. Nevertheless, for a period of two years Respondent has disseminated or caused to be disseminated promotional materials and statements for the Dentrix G5 software that emphasize the product's ability to encrypt patient data and help dentists meet regulatory obligations related to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), including but not limited to the following statements:

A. "The database also provides new encryption capabilities that can help keep patient records safe and secure. And of course, encryption plays a key role in your efforts to stay compliant with HIPAA security standards."
(Dentrix G5 brochure).

B. "Henry Schein is pleased to announce the release of Dentrix G5. G5 stores information in an SQL database, which . . . offers improved protection by storing your patient data in an encrypted format."
(eNewsletter Article).

C. "The SQL database also offers improved protection by storing customer data in an encrypted format. With ever-increasing data protection regulations, Dentrix G5 provides an important line of defense for both patient and practitioner."
(eNewsletter Article).

D. "With the release of Dentrix G5, Dentrix now stores information in an SQL database, which delivers several distinct benefits for your practice, including improved data access speed and improved data protection by storing customer data in an encrypted format. With medical professionals under strict regulatory obligations to protect their patients' personal health information, the new Dentrix G5 database provides an important line of defense for both patient and practitioner."
(Dentrix Magazine).

E. "Dentrix versions prior to G5 relied on the underlying Microsoft operating system and file system safeguard to protect user data. Unfortunately, these were rarely activated by default, and if practices failed to turn them on, their data were at risk to hackers. With Dentrix G5's embedded SQL database, users have the advanced protection they need without burdening them with another system to manage."
(Interview in DentalTown Magazine).

10. On June 10, 2013, the United States Computer Emergency Readiness Team ("US-CERT") issued Vulnerability Note VU#900031, describing the form of data protection used in Dentrix G5 software as a "weak obfuscation algorithm." On June 16, 2013, NIST published a corresponding vulnerability alert.

11. The US-CERT Vulnerability Note stated that the database engine vendor had agreed to re-brand the data protection as "Data Camouflage" so it would not be confused with standard encryption algorithms, such as AES encryption.

12. Despite receiving notice of the US-CERT Vulnerability Note and the database vendor's decision to re-brand in June 2013, for an additional seven months, Respondent continued to disseminate marketing materials stating that Dentrix G5 "encrypts" patient data and offers "encryption."

13. The facts set forth in Paragraphs 7 and 10 would be material to dentists' purchase of Dentrix G5. An attacker who unmasks patients' sensitive personal information could subject patients to the unanticipated disclosure of personal information or use that information to commit identity theft, medical identity theft, or other harms. If dentists were aware that Dentrix G5 used a form of data protection that was more vulnerable than widely-used, industry standard encryption algorithms, they may have chosen to purchase another product.

14. The facts set forth in Paragraphs 7, 8, and 10 would also be material to dentists' use of Dentrix G5. For instance, without knowing that Dentrix G5 provided only minimal protection for their patients' sensitive personal information, dentists may not take other reasonable and commercially available steps to protect patients' sensitive personal information.

15. Moreover, the facts set forth in Paragraphs 7, 8, and 10 would be material to dentists responding to a data breach. For example, in the event of a breach, 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. Even if a dentist does notify patients, the

dentist may misinform patients about their risk of identity theft by telling them that the lost data was "encrypted."

16. Finally, in January 2014, following a series of online media reports criticizing the company's failure to amend its encryption claims, Respondent published the following statement in the Spring 2014 issue of Dentrix Magazine:

> "Available only in Dentrix G5, we previously referred to this data protection as encryption. Based on further review, we believe that referring to it as a data masking technique using cryptographic technology would be more appropriate."

17. Respondent concurrently revised an array of its marketing materials replacing references to "encryption" or "encryption capabilities" with references to "a data masking technique using cryptographic technologies." Respondent also added language to many of its marketing materials warning users that this data masking technique "helps to supplement, not replace" a dentist's own security measures.

18. Aside from revising its marketing materials as described, Respondent did not take any additional steps to alert dentists who purchased Dentrix G5 prior to January 2014, that the software used a less complex algorithm to protect patient data than a standard encryption algorithm such as AES encryption.

Violations of Section 5

Count I
Deceptive Claims of Encryption – Industry-Standard

19. Through the means described in Paragraphs 5, 9, and 12 Respondent has represented, directly or indirectly, expressly or by implication, that Dentrix G5 provides industry-standard encryption.

20. In truth and in fact, as described in Paragraphs 7, 10, and 11, Dentrix G5 used technology that was less secure than industry-standard encryption. Therefore, the representation set forth in Paragraph 19 was false or misleading.

Count II
Deceptive Claims of Encryption – Regulatory Obligations

21. Through the means described in Paragraphs 5, 9, and 12 Respondent has represented, directly or indirectly, expressly or by implication, that Dentrix G5 helps dentists protect patient data, as required by HIPAA.

22. In truth and in fact, as described in Paragraphs 7, 8, 10, and 11, Dentrix G5 used technology that was not capable of helping dentists protect patient data, as required by HIPAA. Therefore, the representation set forth in Paragraph 21 was false or misleading.

23. The acts and practices of Respondent as alleged in this complaint constitute unfair or deceptive acts or practices, in or affecting commerce in violation of Section 5(a) of the Federal Trade Commission Act.

THEREFORE, the Federal Trade Commission this twentieth day of May, 2016, has issued this complaint against Respondent.

By the Commission.

Donald S. Clark
Secretary

SEAL: