***In the Matter of Lenovo (United States) Inc.,* Docket No. C-4636 (2017)**

Lenovo, one of the world’s largest computer manufacturers, began selling certain laptop models to U.S. customers in august 2014. The laptops contained pre-installed software called VisualDiscovery that interfered with how a user’s browser interacted with different websites. That is, whenever users hovered their cursor over a similar looking product on a website, VisualDiscovery delivered pop-up ads from the retail partners of the software developer company Superfish. To make the delivery possible, the software intercepted and collected information that is being exchanged between the users’ browser and the websites they visited, including encrypted sites. The FTC alleged that the technique deployed by VisualDiscovery to deliver ads allowed it to access consumer’s personal information without their knowledge or consent. The transmitted sensitive information includes login credentials, SSNs, medical information, and financial and payment information. The FTC also alleged that Lenovo’s failure to disclose VisualDiscovery’s technique to collect and transfer consumer internet browsing data to Superfish as an unfair and deceptive practice.

Key Lesson: Lenovo failed to take adequate measures to assess and address the security risks created by a third-party software pre-installed on its laptops. The company could have avoided this problem by discovering the software’s security vulnerabilities before preinstallation by implementing readily available and relatively low-cost security measures. The company should have also requested the third-party’s security policies, procedures, and practices, including testing done by the company during the software development process. Lenovo should have also assessed the developer’s compliance with data security standards and its measures to protect the consumer’s personal information.

References

<https://www.ftc.gov/system/files/documents/cases/1523134_c4636_lenovo_united_states_complaint.pdf>

<https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2017-overview-commissions-enforcement-policy-initiatives-consumer/privacy_and_data_security_update_2017.pdf>

***In the Matter of Henry Schein Practice Solutions, Inc.,* Docket No. C-4575 (2016)**

Henry Schein Practice Solutions, advertises, sell, and distributes leading office management software for dental practices, including the Dentrix G5 software. The software enables dentists to perform tasks such as gathering patient data, submitting patient insurance claims, sending appointment reminders, and processing payments. Dentists also use the software to collect and store patient’s sensitive personal information, including SSN, driver license number, and other personally identifiable information. For a period of two years, the company falsely advertised the level of encryption it provided (compliant with HIPAA security standards) to protect patient data even though the database engine vendor informed the company that the software uses a proprietary algorithm that hasn’t been tested. Before releasing the product, the company was also aware of the NIST recommended encryption algorithm, AES.

Consequently, the US-CERT issued a vulnerability note. Despite receiving the note and the Vendor’s decision to re-brand the database, the company continued to market for an additional seven months. After a series of media reports criticizing the company’s failure, it revised its marketing materials by replacing “encryption” with “cryptographic technologies”. However, the FTC followed up after the company didn’t take any steps to alert dentists who purchased the software about the level of protection the product provided. The FTC alleged that the company marketed the software with deceptive claims that it offered industry-standard encryption of sensitive personal information. Consequently, Henry Schein agreed to pay $250,000 to settle charges for its false advertisement.

*Key Lesson:* If software that handles sensitive personal information is not protected by strong encryption (according to NIST guidelines), and that US-CERT informs the provider that the database is vulnerable, the company should take measures before FTC complaint follows.

References

<https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2016/privacy_and_data_security_update_2016_web.pdf>

<https://www.ftc.gov/system/files/documents/cases/160523hspscmpt.pdf>