PREPARED STATEMENT OF

THE FEDERAL TRADE COMMISSION

on

Opportunities and Challenges in Advancing Health Information Technology

Before the

HOUSE OVERSIGHT AND GOVERNMENT REFORM SUBCOMMITTEES ON INFORMATION TECHNOLOGY AND HEALTH, BENEFITS, AND ADMINISTRATIVE RULES

Washington, D.C.

March 22, 2016

I. I

health IT sector. Many of the entities creating these new consumer facing products and services are not covered by the Health Insurance Portability and Accountability Act, or HIPAA, which only provides protections for health information held or generated by certain “covered entities” – namely health care providers, health plans, and health care clearinghouses, and their business associates. The entities creating these new products are, however, within the FTC’s jurisdiction in most instances. As the nation’s foremost consumer protection agency, the FTC is committed to protecting health information collected by these entities. The Commission has engaged in substantial efforts over the years to promote data security and privacy in this area through civil law enforcement, policy initiatives, and business and consumer education. This testimony provides an overv0 Tw 2kI2 Tc -24(f)-1(o)i d herv cause substantial injury to consumers that is neither reasonably avoidable by consumers nor outweighed by countervailing benefits to consumers or to competition, those practices can be unfair and violate Section 5.[5]

The FTC's Section 5 authority extends to both HIPAA and non-HIPAA covered entities,[6] though generally this authority does not reach nonprofit entities or practices that are in the business of insurance to the extent that such business is regulated by state law.[7] The FTC Act is currently the primary federal statute applicable to the privacy and security practices of businesses that collect individually identifiable health information where those entities are not covered by HIPAA.

One recent example of FTC enforcement involving health information is the Commission's settlement with medical billing company PaymentsMD, LLC and its former CEO,

F.T.C. 110, 174 (1984).

[5] See Federal Trade Commission Policy Statement on Unfairness, appended to Int'l Harvester Co., 104 F.T.C. 949, 1070 (1984) ("FTC Unfairness Statement"); 15 U.S.C. § 45(n). In addition to its FTC Act enforcement, Congress in 2009 directed the FTC to implement a breach notification rule for certain web-based businesses not covered by HIPAA that provide or interact with personal health records. 16 C.F.R. Part 318. The FTC's Rule requires these businesses to notify individuals, the FTC, and in some cases, the media when there is a breach of unsecured, electronic health information. In addition, the Rule requires service providers to these entities to notify them in case of a breach.

[6] The Department of Health and Human Services (HHS) and the FTC have worked closely in areas of concurrent jurisdiction, as they have common interests in ensuring the privacy and security of health information for individuals, whether that health information is within or outside the scope of HIPAA. For example, FTC staff collaborated with HHS's Office for Civil Rights to bring a set of cases involving

Michael C. Hughes.[8] The complaint alleged that the company deceived thousands of consumers to data, the need for reasonable and appropriate security, and the types of security failures that raise concerns.[11]

An example of FTC data security enforcement in the health area is the FTC's settlement with GMR Transcription Services, Inc., and its owners for violations of Section 5.[12] According to the complaint, GMR provides audio file transcription services for their clients, which include health care providers, and relies on service providers and independent typists to perform this work. The complaint charged that GMR exchanged audio files and transcripts with customers and typists by loading them on a file server. As a result of GMR's alleged failure to implement reasonable and appropriate security measures and to ensure that its service providers also implemented reasonable and appropriate security, at least 15,000 files containing sensitive personal information – including consumers' names, birthdates, and medical histories – were available to anyone on the Internet. The Commission's order resolving the case prohibits GMR from making misrepresentations about privacy or security, and requires the company to implement a comprehensive information security program and undergo independent audits for 20 years.

More recently the FTC settled an action against Henry Schein Practice Solutions, Inc. According to the complaint, Henry Schein, a provider of office management software for dental practices, misrepresented that its software provided industry-standard encryption of sensitive patient information.[13] The Commission's proposed order requires Henry Schein to pay $250,000

[11] See Commission Statement Marking the FTC's 50th Data Security Settlement, Jan. 31, 2014, available at http://www.ftc.gov/system/files/documents/cases/140131gmrstatement.pdf.

[12] GMR Transcription Servs., Inc., No. C-4482 (F.T.C. Aug. 14, 2014) (decision and order), available at https://www.ftc.gov/enforcement/cases-proceedings/122-3095/gmr-transcription-services-inc-matter.

[13] Henry Schein Practice Solutions, Inc., No. 1423161 (F.T.C. Jan. 5, 2016) (complaint and proposed consent order), available at https://www.ftc.gov/enforcement/cases-proceedings/142-3161/henry-schein-practice-solutions-inc-matter.

as an equitable remedy. The proposed order also prohibits Henry Schein from making misrepresentations about security and requires the company to notify all of its customers who purchased the software during the period when it made the allegedly misleading statements.[14]

B. Policy Initiatives

The Commission also undertakes policy initiatives to promote privacy and data security, including by hosting workshops on emerging business practices and technologies affecting consumer data, and coordinating, where appropriate, with other agencies. This testimony describes three examples of such initiatives relating to the privacy and security of health information.

First, on May 7, 2014, the Commission hosted a seminar on Consumer Generated and Controlled Health Data to examine the greater role consumers are taking in managing and generating their own health data, including through apps, connected health and fitness devices, and websites that allow consumers to share information with others who have the same health conditions.[15] During the event, FTC staff presented a snapshot showing the data-sharing practices of twelve health and fitness apps, including two apps associated with wearable devices. The snapshot revealed that the apps collect and transmit information to third parties, including device information, consumer-specific identifiers, unique device IDs, unique third-party IDs, and consumer information such as exercise routines, dietary habits, and symptom searches.

The seminar also brought together a diverse group of stakeholders to discuss issues such as the benefits arising from the movement of health data outside the traditional medical provider context, the types of products and services consumers use to generate and control their health

[14] Id.

[15] See http://www.ftc.gov/news-events/events-calendar/2014/05/spring-privacy-series-consumer-generated-controlled-health-data.

data, consumers’ expectations regarding privacy and security protections, and the actions some companies take to protect consumers’ privacy and security. FTC staff followed up with two blog posts providing additional guidance for businesses innovating in this area.[16]

Second, at the beginning of 2015, the FTC released a staff report about the Internet of Things (“IoT”).[17] Among other areas, the report examined the growth of increasingly connected medical devices and health and fitness products, ranging from casual wearable fitness devices to connected insulin pumps. The report recommends, among other things, that companies developing IoT products secure

businesses in various industries.[22] Our goal is to help companies reduce security risks by starting with smart data security practices. In addition, the BCP business blog, which has over 50,000 email subscribers, regularly explains FTC cases and illustrates lessons learned in plain language. The Commission also has released articles directed towards particular non-legal audiences regarding data security.[23] For example, the FTC has specific tips to help mobile app developers build data security in from the start.[24] The FTC also has released business guidance about building security into connected devices.[25]

Recognizing that mobile health app developers are often confused about which legal requirements apply to them, the FTC has undertaken a joint interagency project with HHS to provide guidance on this issue. In cooperation with HHS's ONC, Office for Civil Rights, and Food and Drug Administration, the FTC is developing an interactive tool that uses a series of high-level questions and prompts to show app developers which laws – including HIPAA, the Federal Food, Drug, and Cosmetic Act, the FTC Act, and the FTC's Health Breach Notification Rule — apply to them. Once a developer determines which laws apply, she can use hyperlinks within the tool to access each agency's guidance and learn how to comply with relevant laws. This interactive resource will reside on the FTC's website with links from other

[22] See Start with Security – San Francisco, available at https://www.ftc.gov/news-events/events-calendar/2015/09/start-security-san-francisco; Start with Security – Austin, available at https://www.ftc.gov/news-events/events-calendar/2015/11/start-security-austin; Start with Security – Seattle, available at https://www.ftc.gov/news-events/events-calendar/2016/02/start-security-seattle.

[23] See generally https://www.ftc.gov/tips-advice/business-center.

[24] See Mobile App Developers: Start with Security (Feb. 2013), available at http://business.ftc.gov/documents/bus83-mobile-app-developers-start-security.

[25] See Careful Connections: Building Security in the Internet of Things (Jan. 2015), available at https://www.ftc.gov/tips-advice/business-center/guidance/careful-connections-building-security-internet-things

agencies.In conjunction with this project, the FTC also plans to release additional business guidance to help mobile health app developers build privacy and security into their apps.

III. RECOMMENDATIONS FOR NEXT STEPS

The Commission shares these Subcommittees' concerns about the need to protect the privacy and security of consumers' health data. Although the agency is using a variety of to be caused by the misuse of their data. And although most states have breach notification laws in place, having a strong and consistent national requirement would ensure that all consumers are protected while simplifying compliance by businesses.

Legislation in both areas – data security and breach notification – should give the FTC the ability to seek civil penalties to help deter unlawful conduct, jurisdiction over non-profits, and rulemaking authority under the Administrative Procedure Act. Under current laws, the FTC only has the authority to seek civil penalties for data security violations with regard to children’ online information under the Children’s Online Privacy Protection Act or credit report information under the Fair Credit Reporting Act.[28] To help ensure effective deterrence, we urge Congress to allow the FTC to seek civil penalties for all data security and breach notice violations in appropriate circumstances. Likewise, enabling the FTC to bring cases against non-profits[29] would help ensure that whenever personal information is collected from consumers, entities that maintain such data adequately protect it.[30]

IV. CONCLUSION

Thank you for the opportunity to provide the Commission’s views on Opportunities and Challenges in Advancing Health Information Technology. The FTC remains committed to protecting consumer health information and we look forward to continuing to work with Congress on this critical issue.

[28] The FTC can also seek civil penalties for violations of administrative orders. 15 U.S.C. § 45(l).

[29] Non-profits are generally outside the FTC’s jurisdiction under the FTC Act. 15 U.S.C. §§ 44 & 45(a).

[30] A substantial number of reported breaches have involved non-profit universities and health systems. *See* Privacy Rights Clearinghouse Chronology of Data Breaches (listing breaches including breaches at