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. INTRODUCTION

Chairmen Hurd and Jordan, Ranking Members Kelly and Cartwright, and members of the Subcommittees, I am Jessica Rich, Director of the Bureau of Consumer Protection at the Federal Trade Commission ("FTC" or "Commission").[1] I appreciate the opportunity to present the Commission's testimony on Opportunities and Challenges in Advancing Health Information Technology.

Consumers are increasingly taking a more active role in managing their health data. It seems like every day a company announces a new health-related app, device, or service. There are apps that allow consumers to track their diet and exercise habits, devices that help consumers track their glucose levels, and websites where patients with the same condition share information. In addition, consumers are downloading their medical information into personal health records and using this information to make decisions about their health.

Much of this activity now takes place outside of doctors' offices and other traditional medical contexts, and the tremendous growth in this area is not slowing down. Many of these products and services offer consumers substantial benefits in the form of increased consumer engagement in their health and fitness, reduced healthcare costs, and improved outcomes. But these products and services also raise privacy and security concerns. Consumers may be concerned about the unauthorized disclosure of their health data, which they often regard as highly sensitive and private. In addition, data breaches involving health information can cause serious harms to consumers, including fraud and medical identify theft. Finally, if consumer health data is used for unanticipated, harmful purposes, consumers could lose confidence in the

[1] This written statement presents the views of the Federal Trade Commission. My oral statements and responses to questions are my own and do not necessarily reflect the views of the Commission or of any Commissioner.

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 overview of the Commission's recent efforts and provides recommendations for next steps.

II. THE COMMISSION'S PRIVACY AND DATA SECURITY WORK IN THE HEALTH AREA

A. Law Enforcement

The FTC enforces several statutes and rules that impose obligations upon businesses to protect consumer data.[2] The Commission's primary authority is Section 5 of the FTC Act, which prohibits unfair or deceptive acts or practices in or affecting commerce.[3] If a company makes materially misleading statements or omissions about a matter, including privacy or data security, and such statements or omissions are likely to mislead reasonable consumers, they can be deceptive in violation of Section 5.[4] Further, if a company's practices cause or are likely to

[2] 15 U.S.C. § 45(a) (Section 5 of the FTC Act); 15 U.S.C. §§ 6801-6809 (GLBA); 15 U.S.C. § 1681 (FCRA); 15 U.S.C. §§ 6501-6506 (COPPA) and 16 C.F.R. Part 312 (COPPA Rule).

[3] 15 U.S.C. § 45(a).

[4] *See* Federal Trade Commission Policy Statement on Deception, *appended to Cliffdale Assocs., Inc.*, 103

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 faulty data security practices that implicated both HIPAA and the FTC Act. *See Rite Aid Corporation*, No. C-4308 (F.T.C. Nov. 12, 2010) (decision and order), *available at:* https://www.ftc.gov/enforcement/cases-proceedings/072-3121/rite-aid-corporation-matter; *see also CVS Caremark Corporation*, No. C-4259 (F.T.C. June 18, 2009) (decision and order), *available at:* https://www.ftc.gov/enforcement/cases-proceedings/072-3119/cvs-caremark-corporation-matter.

[7] 15 U.S.C. §§ 44 & 45(a). The FTC does not have jurisdiction under the FTC Act over most non-profit organizations, although it does have jurisdiction over sham charities or other non-profits that in actuality operate for profit. The FTC's Section 5 jurisdiction also does not extend to banks, savings and loan institutions, Federal credit unions, common carriers, air carriers, or packers and stockyard operators.

Michael C. Hughes.[8] The complaint alleged that the company deceived thousands of consumers who signed up for an online billing portal by failing to adequately inform them that the company would seek highly detailed medical information about them from pharmacies, medical labs, and insurance companies. Specifically, the company allegedly used the sign-up process for its "Patient Portal" – where consumers could view their billing history – to deceptively seek consumers' consent to collect detailed medical information from other entities for use in a separate Patient Health Report service.[9] The Commission's order prohibits PaymentsMD and Hughes from making future privacy misrepresentations. It also requires respondents to destroy any information collected as a result of its allegedly deceptive sign-up process, and obtain consumers' affirmative express consent before collecting health information about a consumer from a third party.[10]

The FTC has also used its Section 5 authority to bring enforcement actions against companies that fail to maintain reasonable and appropriate data security practices regarding consumer data, including health data. Since 2001, the Commission has obtained settlements in approximately 60 cases challenging such failures. In investigating these cases, the FTC determines whether a company's data security measures are reasonable and appropriate in light of the sensitivity and volume of information it holds, the size and complexity of its data operations, and the cost of available tools to improve security and reduce vulnerabilities. The Commission orders obtained in these cases have halted harmful data security practices; required companies to provide strong protections for consumer data; and raised awareness about the risks

[8] *PaymentsMD, LLC*, No. C-4505 (F.T.C. Jan. 27, 2015) (decision and order), a*vailable at:* https://www.ftc.gov/enforcement/cases-proceedings/132-3088/paymentsmd-llc-matter.
[9] *Id.*
[10] *Id.*

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 personally identifiable information and device functionality by, for example, conducting risk assessments, hiring and training appropriate personnel, monitoring access controls, and utilizing technologies such as encryption.

Third, FTC staff have worked with the Department of Health and Human Services' (HHS) Office of the National Coordinator for Health Information Technology (ONC) on several initiatives. For example, FTC staff provided comments on the Federal Health IT Strategic Plan, a coordinated effort among more than thirty-five federal agencies to advance the collection, sharing, and use of electronic health information in a manner that protects privacy and security in order to improve health care, individual and community health, and research.[18] FTC staff also

---

[16] *See* Using Consumer Health Data? (Apr. 2015*), available at* https://www.ftc.gov/news-events/blogs/business-blog/2015/04/using-consumer-health-data; Using Consumer Health Data: Some Considerations for Companies (Apr. 2015), *available at*, https://www.ftc.gov/news-events/blogs/business-blog/2015/04/using-consumer-health-data-some-considerations-companies.

[17] FTC Staff Report, *Internet of Things: Privacy and Security in a Connected World* (Jan. 2015), *available at* https://www.ftc.gov/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things Commissioner Ohlhausen issued a concurring statement. *See* https://www.ftc.gov/sites/default/files/documents/public_statements/remarks-commissioner-maureen-k.ohlhausen-ftc-internet-things-workshop/131119iotspeech.pdf; Commissioner Wright dissented to the release of the report. *See* https://www.ftc.gov/system/files/documents/public_statements/620701/150127iotjdwstmt.pdf.

[18] *See* https://www.healthit.gov/sites/default/files/9-5-federalhealthitstratplanfinal_0.pdf. FTC staff also commented on ONC's Shared Nationwide Interoperability Roadmap for Health Information Technology

participated as ex officio members in the Privacy and Security Workgroup of ONC's Health IT Policy Committee which, among other things, considered the intersection of big data and healthcare.[19]

C. Consumer Education and Business Guidance

The Commission also promotes better data security and privacy practices through consumer education and business guidance. On the consumer education front, the Commission manages a consumer information website and blog with over 300 articles and blog posts related to privacy and security.[20] The website gets over 18 million visitors each year, and the blog has over 100,000 email subscribers. In addition, as part of IdentityTheft.gov, the FTC provides customized advice for victims of medical identity theft. Among other things, these materials help consumers determine if they have been victims of identity theft, how to correct mistakes in their medical records, how to protect their medical information, and how to check for other identity theft problems.

The Commission directs its outreach to businesses as well. "Start with Security" is the Commission's latest effort to educate businesses about information security. This initiative kicked off with a business guide that highlighted what businesses could learn from more than 50 data security cases brought by the FTC in recent years.[21] The FTC is now following up with conferences and webinars around the country, aimed at educating small- and medium-sized

---

Systems, a plan to guide the future development of the nation's health IT infrastructure. *See* https://www.ftc.gov/system/files/documents/advocacy_documents/ftc-staff-comment-office-national-coordinator-health-information-technology-regarding-its-draft/1504-roadmaphealth.pdf.

[19] *See* Health Big Data Recommendations (August 2015), *available at* www.healthit.gov/sites/faca/files/HITPC_Health_Big_Data_Report_FINAL.pdf.

[20] *See generally* https://www.consumer.ftc.gov/.

[21] *See Start with Security: A Guide for Business* (June 2015), *available at* https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business.

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, he or 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 tools to promote better privacy and security of this data, additional tools would enhance the agency's ability to protect consumers. To this end, the Commission reiterates its longstanding, bipartisan call for federal legislation[26] that would (1) strengthen its existing data security authority and (2) require companies, in appropriate circumstances, to provide notification to consumers when there is a security breach.[27] Reasonable and appropriate security practices are critical to preventing data breaches and protecting consumers from identity theft and other harm. Where breaches occur, notifying consumers helps them protect themselves from any harm that is likely

---

[26] *See, e.g.*, Prepared Statement of the Federal Trade Commission, "Privacy and Data Security: Protecting Consumers in the Modern World," Before the Senate Committee on Commerce, Science, and Transportation, 112th Cong., June 29, 2011, *available at* http://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-federal-trade-commission-privacy-and-data-security-protecting-consumers-modern/110629privacytestimonybrill.pdf; Prepared Statement of the Federal Trade Commission, "Data Security," Before Subcommittee on Commerce, Manufacturing, and Trade of the House Committee on Energy and Commerce, 112th Cong., June 15, 2011, *available at* http://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-federal-trade-commission-data-security/110615datasecurityhouse.pdf; FTC, *Security in Numbers, SSNs and ID Theft* (Dec. 2008), *available at* http://www.ftc.gov/sites/default/files/documents/reports/security-numbers-social-security-numbers-and-identity-theft-federal-trade-commission-report/p075414ssnreport.pdf; President's Identity Theft Task Force, *Identity Theft Task Force Report* (Sept. 2008), *available at* http://www.ftc.gov/sites/default/files/documents/reports/presidents-identity-theft-task-force-report/081021taskforcereport.pdf.

[27] HIPAA has a breach notification rule, but HIPAA only applies to certain "covered entities" and their business associates as discussed above. Although the FTC has its own health breach notification rule, *see supra* n.5, this Rule is narrow in scope in accordance with the 2009 legislation and would not cover, for example, many health websites or online newsletters. Nor would it cover health apps or devices that are not vendors of "personal health records" or "PHR-related entities" as defined by the Rule. *See* 16 C.F.R. § 318(2)(f) and (j). In particular, the Rule defines a "personal health record" as information that "can be drawn from multiple sources," such as a doctor's office.

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's 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 non-profits, educational institutions, and health facilities), *available at* http://www.privacyrights.org/data-breach/new.