PREPARED STATEMENT OF THE FEDERAL TRADE COMMISSION

"Hearing on Improving Data Security at Consumer Reporting Agencies"

Before the

COMMITTEE ON OVERSIGHT AND REFORM

SUBCOMMITTEE ON ECONOMIC AND CONSUMER POLICY

UNITED STATES HOUSE OF REPRESENTATIVES

WASHINGTON, DC

MARCH 26, 2019

I. INTRODUCTION

Chairman Krishnamoorthi, Ranking Member Cloud, and members of the Subcommittee, my name is Andrew Smith, and I am the Director of the Bureau of Consumer Protection at the Federal Trade Commission ("Commission" or "FTC").[1] I appreciate the opportunity to appear before you today to discuss the Commission's role in oversight of consumer reporting agencies' data security practices.

This testimony provides an overview of the Commission's efforts to promote data security, especially as they relate to CRAs, and explains further the Commission's support for federal data security legislation.

II. THE COMMISSION'S DATA SECURITY PROGRAM

A. Law Enforcement

For nearly two decades, the FTC has been the nation's leading data security enforcement agency, litigating or settling more than 60 data security cases. The Commission is the nation's primary data security regulator and enforces several statutes and rules that impose data security requirements on companies across a wide spectrum of industries, including CRAs. In 2017, the Commission took the unusual step of publicly confirming its investigation into the Equifax data breach due to the scale of public interest in the matter.

Since 2001, the Commission has undertaken substantial efforts to promote data security in the private sector through enforcement of Section 5 of the FTC Act, which prohibits unfair or deceptive acts or practices, such as businesses making false or misleading claims about their data security procedures, or failing to employ reasonable security

[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.

measures.[2] Further, the Commission's Safeguards Rule, which implements the Gramm-Leach-Bliley Act ("GLB Act"), requires certain non-bank financial institutions – including CRAs – to safeguard nonpublic personal information by developing, implementing, and maintaining a comprehensive information security program.[3] The FTC recently proposed more detailed requirements for what should be included in the comprehensive information security program mandated by the Safeguards Rule, and is currently seeking comment on its proposals.[4] Finally, the Fair Credit Reporting Act ("FCRA") requires CRAs to use reasonable procedures to ensure that the entities to which they provide consumer reports have a permissible purpose for receiving that information,[5] and also requires the secure disposal of consumer report information.[6]

The FTC has significant experience with enforcing data security laws against CRAs. In 2006, the FTC brought the seminal *Choicepoint* case against a CRA that allegedly sold consumer reports to identity thieves who did not have a permissible purpose to obtain the information under the FCRA, failed to employ reasonable measures to secure the personal information it collected, and misrepresented its security practices.[7] The complaint charged that ChoicePoint failed to monitor subscribers even after receiving subpoenas from law enforcement alerting it to fraudulent activity. The settlement included injunctive relief, as

---

[2] 15 U.S.C. § 45(a). If a company makes materially misleading statements or omissions about a matter, including data security, and such statements or omissions are likely to mislead reasonable consumers, they can be found to be deceptive in violation of Section 5. Further, if a company's data security practices cause or are likely to 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 found to be unfair in violation of Section 5.
[3] 16 C.F.R. Part 314, implementing 15 U.S.C. § 6801(b).
[4] Press Release, *FTC Seeks Comment on Proposed Amendments to Safeguards and Privacy Rules* (Mar. 5, 2019), https://www.ftc.gov/news-events/press-releases/2019/03/ftc-seeks-comment-proposed-amendments-safeguards-privacy-rules.
[5] 15 U.S.C. § 1681e.
[6] *Id.* § 1681w. The FTC's implementing rule is at 16 C.F.R. Part 682.
[7] *U.S. v. Choicepoint, Inc.*, No. 1:06-cv-00198-GET (N.D. Ga. filed Jan. 30, 2006), https://www.ftc.gov/enforcement/cases-proceedings/052-3069/choicepoint-inc.

well as $10 million in civil penalties—the largest FCRA civil penalty in FTC history—and $5 million in consumer redress. A few years later, the FTC settled another action against the company when it suffered a data breach because it turned off a key electronic security tool used to monitor access to one of its databases, in violation of the 2006 order.[8]

The Commission has also brought actions against companies for failing to dispose of consumer report information securely. For example, in the *PLS Financial Services* case, the FTC alleged that the company violated the FCRA Disposal Rule by improperly disposing of consumer report information, violated the GLB Safeguards Rule by failing to develop and use safeguards to protect consumer information, and violated the FTC Act by misrepresenting that it had implemented reasonable measures to protect sensitive consumer information.[9] The settlement included injunctive relief and approximately $100,000 in civil penalties.

B. Policy Initiatives

Law enforcement is not the Commission's only tool. The FTC also uses policy initiatives, such as workshops, reports, and rulemaking, to promote data security, including among CRAs. For example, in October 2018, Commission staff issued its perspective on the FTC's December 2017 Informational Injury Workshop, which explored the injuries consumers may suffer from privacy and security incidents such as data breaches or unauthorized disclosure of data.[10] In December, the FTC held a hearing on data security as

---

[8] *U.S. v. Choicepoint, Inc.*, No. 1:06-cv-00198-JTC (N.D. Ga. filed Oct. 19, 2009), https://www.ftc.gov/enforcement/cases-proceedings/052-3069/choicepoint-inc.

[9] *U.S. v. PLS Financial Services, Inc.*, No. 112-cv-08334 (N.D. Ill. filed Oct. 17, 2012), https://www.ftc.gov/enforcement/cases-proceedings/1023172/pls-financial-services-inc-et-al.

[10] FTC Staff Perspective, *FTC Informational Injury Workshop: BE and BCP Staff Perspective* (Oct. 2018), https://www.ftc.gov/system/files/documents/reports/ftc-informational-injury-workshop-be-bcp-staff-perspective/informational_injury_workshop_staff_report_-_oct_2018_0.pdf.

part of its series of *Hearings on Competition and Consumer Protection in the 21st Century*.[11] Participants discussed a variety of data security-related topics, including the prevalence and consequences of data breaches, incentives to invest in data security, consumer demand for security, data security assessments, and whether the FTC's current authority is sufficient to address data security harms.[12] This hearing, like the others in the series, has yielded important information about business and technological changes that affect pressing consumer protection issues.

Finally, where Congress has provided the Commission with rulemaking authority related to data security, we will use that authority when warranted. As mentioned above, the Commission recently proposed changes to the Safeguards Rule under the GLB Act, and is soliciting public comment on those proposed amendments. The Safeguards Rule, originally issued in 2002, requires financial institutions within the FTC's jurisdiction – including CRAs – to implement reasonable, process-based safeguards to protect personal information in their control. When originally issued, the Safeguards Rule was groundbreaking and served as a model for other risk-based rulemaking. These proposed revisions are intended to retain the process-based approach of the original Rule while providing financial institutions with more certainty as to the FTC's data security expectations, and we welcome comments from interested parties.

C. Business Guidance and Consumer Education

---

[11] Press Release, *FTC Announces Sessions on Consumer Privacy and Data Security as Part of Its Hearings on Competition and Consumer Protection in the 21st Century* (Oct. 26, 2018), https://www.ftc.gov/news-events/pressreleases/2018/10/ftc-announces-sessions-consumer-privacy-data-security-part-its.

[12] *FTC Hearing on Competition and Consumer Protection in the 21st Century* – December 2018, https://www.ftc.gov/news-events/events-calendar/ftc-hearing-competition-consumer-protection-21st-centurydecember-2018 (last visited Mar. 14, 2019).

Finally, the FTC provides extensive guidance on data security to businesses and consumers alike. As to business guidance, the agency's goal is to provide information to help businesses protect the data in their care and understand what practices may violate the laws the FTC enforces. The FTC provides general business education about data security issues, as well as specific guidance on emerging threats.

In 2015, for example, the FTC launched its *Start with Security* initiative, which includes a guide for businesses,[13] as well as 11 short videos,[14] that discuss ten important security topics and give advice about specific security practices for each. In 2016, the FTC published a business advisory on how the National Institute of Standards and Technology Cybersecurity Framework applies to the FTC's data security work[15] and released an update to *Protecting Personal Information: A Guide for Business*, which was first published in 2007.[16] In 2017, the FTC released its *Stick with Security* initiative offering additional insights into the *Start with Security* principles, based on the lessons of law enforcement actions, closed investigations, and experiences companies have shared about data security in their business.[17]

In addition to data security guidance, the FTC provides business guidance related to data breaches. In September 2016, the FTC released *Data Breach Response: A Guide for*

---

[13] *Start with Security: A Guide for Business* (June 2015), https://www.ftc.gov/tips-advice/businesscenter/guidance/start-security-guide-business.
[14] FTC Videos, *Start with Security* (2015-2016), https://www.ftc.gov/newsevents/audio-video/business.
[15] FTC Business Blog, *The NIST Cybersecurity Framework and the FTC* (Aug. 31, 2016), https://www.ftc.gov/news-events/blogs/business-blog/2016/08/nist-cybersecurity-framework-ftc.
[16] *Protecting Personal Information: A Guide for Business* (Oct. 2016), https://www.ftc.gov/tipsadvice/business-center/guidance/protecting-personal-information-guide-business.
[17] FTC Business Blog, *Stick with Security: A Business Blog Series* (Oct. 2017), https://www.ftc.gov/tips-advice/business-center/guidance/stick-security-business-blog-series.

Business,[18] and a related video, which describes immediate steps companies should take when they experience a data breach, such as taking breached systems offline, securing physical areas to eliminate the risk of further harm from the breach, and notifying consumers, affected businesses, and law enforcement. The guide also includes a model data breach notification letter businesses can use to get started.

The FTC also provides businesses with specific guidance on emerging threats. For example, most recently the FTC released a staff perspective and related blog post to help businesses prevent phishing scams.[19] Following a workshop,[20] the FTC published a blog post describing ransomware,[21] how to defend against it, and essential steps to take if businesses become victims.[22] Further, the FTC develops targeted guidance for companies in specific industries. For example, staff developed specific security guidance for debt buyers and sellers.[23]

The Commission also educates consumers on data security in a variety of ways. For example, the FTC website highlights timely security issues—recent examples include tax identity theft, a Netflix phishing scam, tips on buying internet-connected smart toys, and the aftermath of the Marriott data breach.[24] The FTC may also provide in-depth materials on a

---

[18] *Data Breach Response: A Guide for Business* (Oct. 2016), https://www.ftc.gov/tips-advice/businesscenter/guidance/data-breach-response-guide-business.
[19] FTC Staff Perspective, *Businesses Can Help Stop Phishing and Protect Their Brands Using Email Authentication* (Mar. 2017), https://www.ftc.gov/reports/businesses-can-help-stop-phishing-protect-their-brands-usingemail-authentication-ftc-staff; FTC Business Blog, *Want to stop phishers? Use email authentication* (Mar. 3, 2017), https://www.ftc.gov/news-events/blogs/business-blog/2017/03/want-stop-phishers-use-emailauthentication.
[20] *Fall Technology Series: Ransomware* (Sept. 7, 2016), https://www.ftc.gov/news-events/eventscalendar/2016/09/fall-technology-series-ransomware.
[21] Ransomware is malicious software that infiltrates computer systems or networks and uses tools like encryption to deny access or hold data "hostage" until the victim pays a ransom.
[22] FTC Business Blog, *Ransomware – A Closer Look* (Nov. 10, 2016), https://www.ftc.gov/newsevents/blogs/business-blog/2016/11/ransomware-closer-look.
[23] *Buying or selling debts? Steps for keeping data secure* (Apr. 2015), https://www.ftc.gov/tipsadvice/business-center/guidance/buying-or-selling-debts-steps-keeping-data-secure.
[24] *See generally* FTC Consumer Blog, https://www.consumer.ftc.gov/blog (last visited Mar. 15, 2019).

data security topic of particular concern to consumers. For example, immediately following the Equifax data breach, the agency created a dedicated page on its website with information about fraud alerts, active duty alerts, credit freezes and locks, credit monitoring, and how to reduce the risk of identity theft.[25]

Finally, the FTC assists consumers affected by data breaches through identitytheft.gov. This website allows victims of data breaches to get information on how to protect their personal information, and enables identity theft victims to easily file a complaint with the FTC and get a personalized report that can be used to help communicate with financial companies and CRAs. For victims of tax identity theft, identitytheft.gov helps people file the IRS Identity Theft Affidavit with the IRS – the first-ever digital pathway to do so.

III. DATA SECURITY LEGISLATION

The Commission agrees with the GAO's recommendation that providing the FTC with civil penalty authority for violations of GLB's Safeguards Rule would give the FTC a practical enforcement tool that would benefit consumers. Beyond GLB, however, the Commission has long called for comprehensive data security legislation that would give the agency additional tools.

In particular, the FTC supports data security legislation that would provide the agency with three essential additional authorities: (1) the ability to seek civil penalties effectively to deter unlawful conduct, (2) jurisdiction over non-profits and common carriers, and (3) the authority to issue targeted implementing rules under the Administrative Procedure Act ("APA"). Each of these additional authorities is important to the Commission's efforts to

[25] FTC, *The Equifax Data Breach*, https://www.ftc.gov/equifax-data-breach (last visited Mar. 15, 2019).

combat unreasonable security. When the FTC brings data security cases under the FTC Act or the GLB Safeguards Rule, it cannot obtain civil penalties for first-time violations. To help ensure effective deterrence, we urge Congress to enact legislation to allow the FTC to seek civil penalties for data security violations in appropriate circumstances. Likewise, enabling the FTC to bring cases against non-profits and common carriers is important because these entities often collect sensitive consumer information. Finally, the ability to engage in targeted APA rulemaking authority would enable legal requirements to keep up with business and technological changes.

IV. CONCLUSION

Thank you for the opportunity to provide the Commission's views on data security and CRAs, and thank you to the GAO for its thoughtful report and recommendations. We look forward to continuing to work with Congress and this Committee on these important issues.