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 –

well as $10 million in civil penalties

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://.202 0.3//.20://.202 02 hx.3 2/of 72 1 e12 (0 9.96hu4( )]5 (s)-19 73/v]5

Business,[18]

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.