PREPARED STATEMENT OF THE

FEDERAL TRADE COMMISSION

Before the

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

Permanent Subcommittee on Investigations

UNITED STATES SENATE

WASHINGTON, DC

MARCH 7, 2019

I. INTRODUCTION

Chairman Portman, Ranking Member Carper, and members of the Subcommittee, I am Andrew Smith, Director of the Bureau of Consumer Protection at the Federal Trade Commission ("FTC" or "Commission").[1] I 33.54 -26.15 Smith mid-sized Pmith c(e)4kthurieatapp

Today, the Commission reiterates

necessarily mean that a company's security was unreasonable. Rather, reasonable security requires an ongoing process of assessing and addressing risks. In deciding whether to pursue an action, the Commission considers whether a company's data security measures are reasonable in light of the sensitivity and volume of consumer information it holds, the size and complexity of its operations, and the cost of tools available to reduce data security risks.

Several recent cases illustrate this approach. In a revised settlement with Uber Technologies, Inc.,[11] the FTC charged that the popular ride-sharing company deceived consumers by failing to reasonably secure sensitive consumer data stored in the cloud, despite promises of secure storage. Uber's alleged security failures were numerous: using a single key for full administrative access to consumer data, not requiring two-factor authentication (a widely-used, readily available safeguard in this area), and storing sensitive consumer information in plain readable text in database backups stored in the cloud. In light of these alleged pervasieg (er)-1 0 Tb reecTc 1

sec-14 (at)-4 (i)-4 (e)f.004 Tw [(av)-4 (a

reasonable technical security measures or engaged in reasonable oversight of its service provider, the third party would not have been able to access such sensitive information.

The FTC is currently litigating an action against computer networking equipment manufacturer D-Link, whose alleged inadequate security measures left consumers' wireless routers and internet cameras vulnerable to hackers.[13] Here, too, the FTC is challenging multiple alleged security failures: shipping software with well-known flaws, mishandling a private code-signing key, and storing login credentials in clear text. This action, like the FTC's other data security cases, sends a clear message that the FTC uses its existing tools to the fullest extent to stop unreasonable data security p]TJ -28.9 -2ruab0 (cces)-5 (s)]Toonaben (i)-2 3.9 (e:)]TJ 0 Tc 0 Tw-5 (e5n)

In November, the FTC held a hearing on data security as part of its series of Hearings on Competition and Consumer Protection in the 21st Century.[16] Participants included academics, industry representatives, practitioners, and consumer advocates who discussed a variety of data security-related topics, including

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 Identity Theft report that can be used to help communicate with financial companies and credit reporting agencies. 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

While the Commission uses its existing authorities aggressively, the FTC reiterates its longstanding bipartisan call for comprehensive data security legislation. 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 to effectively deter unlawful conduct, (2) jurisdiction over non-profits and common carriers, and (3) the authority to issue implementing rules under the Administrative Procedure Act ("APA"), as appropriate.[28]

Each of these additional authorities is important to the Commission's efforts to combat unreasonable security. Under current laws, the FTC only has the authority to seek civil penalties for data security violations related to children's online information (under COPPA) or credit report information (under the FCRA).[29] When the FTC brings data security cases under the FTC Act or the GLB Safeguards Rule, it cannot obtain civil penalties for first violations. To help ensure effective deterrence, we urge Congress to enact specific 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. For example, educational institutions often collect

[28] While today's hearing focuses on data security, the Commission recognizes that many aspects of data security intersect with broader questions about consumer data privacy. The Commission urges Congress to consider enacting privacy legislation that would be enforced by the FTC.

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

Social Security numbers and common carriers often collect the contents of consumer communications. Significant breaches have been reported in each of these sectors.[30]

Finally, the ability to engage in targeted APA rulemaking authority would add considerable legal