STATEMENT OF
COMMISSIONER GEOFFREY STARKS

Re: *Data Breach Reporting Requirements*, WC Docket No. 22-21, Report and Order

Unfortunately, we've all been there. You check your mail only to find a letter from a service provider announcing that your sensitive information has been leaked as part of a data breach. And, if it seems like these notifications and announcements are happening more frequently, you're right. According to a recent report, data breaches impacting US organizations are already at an all-time high. There were more breaches in the first three quarters of 2023 than in any prior year.[1] Another report states that the United States saw 1,802 data breaches in 2022 with 422.14 million records exposed and 298 million Americans impacted.[2]

This matters. Sensitive data breaches include the type of information that bad actors can exploit for identify theft, financial fraud and crimes, and scams, placing consumers at risk in a multitude of ways.

Congress recognized this too. Section 222 of the Communications Act gives us clear authority, and carriers a duty, to protect the confidentiality of proprietary information of and relating to consumers and others.[3] We first adopted our data breach rules 16 years ago in 2007, but the intervening years have shown that our data breach rules are badly in need of an update. The amount of data service providers now collect and retain has greatly expanded the risk profile for consumers and their carriers, as does the sophistication of bad actors who are constantly trying to access that data. So, I'm glad that we update our rules today in response to the reality that we need to do more to both protect sensitive consumer data and notify consumers and the authorities when a data breach occurs.

One overdue change is to properly expand the definition of "breach" beyond the intentional access, use, or disclosure of covered data. Many breaches are inadvertent, but harmful nonetheless, and the impact on consumers when their data is disclosed does not turn on the question of intent. At the same time, we recognize that breach notice fatigue is real. To avoid this risk, the Order properly adopts a harm-based notification trigger and an affected consumer trigger threshold that limits the consumer reporting requirement and balances the need for notice with the burden on consumers if harm is unlikely. We should also continue to work with our agency partners to coordinate filing obligations across the government over time, including as the Cybersecurity and Information Security Agency works on their Cybersecurity Incident Reporting rulemaking.

I also agree with the need for providers to encrypt their data, especially sensitive data. I can't emphasize it enough—at a minimum, providers should be encrypting the data they hold as a basic best practice. While we do not require encryption in this item, we adopt encryption as a safe harbor, recognizing it is a critical defense against data breaches and incentivizing providers to embrace it. Consumers trust providers with their most sensitive information, and the marketplace demands that carriers take these widely available steps to protect them, including measures like access controls, firewalls, intrusion detection and prevention, and security audits and updates to further defend against modern cyber threats.

I thank the Chairwoman for working with me on the edits that I suggested to help the item strike

---

[1] Stuart E. Madnick, Ph.D., *The Continued Threat to Personal Data: Key Factors Behind the 2023 Increase*, Dec. 2023, https://www.apple.com/newsroom/pdfs/The-Continued-Threat-to-Personal-Data-Key-Factors-Behind-the-2023-Increase.pdf.

[2] Ani Petrosyan, *Annual number of data compromises and individuals impacted in the United States from 2005 to 2022*, Statista Aug. 29, 2023, https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/.

[3] *See* 47 U.S.C. § 222(a).

the right balance in defining the Personally Identifiable Information (PII) data that needs to be protected and the level of harm that triggers a reporting obligation. Data breaches will continue to be a problem, but by notifying consumers and the government we can take steps to mitigate the harm. I thank the Chairwoman for her leadership in updating our data breach rules and I thank the Commission staff for their hard work on this item. I approve.