Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)
	)
Data Breach Reporting Requirements	) WC Docket No. 22-21

REPLY COMMENTS
OF
WTA – ADVOCATES FOR RURAL BROADBAND

WTA – Advocates for Rural Broadband ("WTA") hereby submits its reply comments with respect to the Commission's *Notice of Proposed Rulemaking* (Data Breach Reporting Requirements), FCC 22-21, released January 6, 2023 in this proceeding (*"NPRM"*).

WTA's primary concern in this proceeding is that the relatively small staffs of its rural local exchange carrier ("RLEC") members retain the flexibility and capability to focus their full attention upon the critical tasks of data and operational recovery after a Customer Proprietary Network Information ("CPNI") data breach incident, and not be overburdened and confused by a variety of differing reporting formats and schedules for the same incident. It urges the Commission to coordinate its data breach reporting requirements and deadlines with those of other federal and state agencies so that the growing number of cybersecurity reporting obligations and timeframes are consistent with each other to the maximum feasible extent.

Definition of "Breach"

WTA reiterates that the existing Section 64.2011(e) definition of "breach" as an intentional action ("when a person, without authorization or exceeding authorization, has intentionally gained access to, used, or disclosed CPNI") is more than sufficient to encompass the

CPNI data breaches that should be reported to and investigated by the Commission, the Federal Bureau of Investigation ("FBI") and the United States Secret Service ("USSS").

WTA opposes extension of the Commission's definition of "breach" for reporting purposes to include: (a) accidental or inadvertent access, use or disclosure of CPNI; or (b) situations where a carrier or third party discovers conduct that could have led to exposure of CPNI even if it has not yet been determined whether such exposure actually occurred.

For WTA members, most accidental or inadvertent incidents are in the nature of an unauthorized employee or visitor overhearing a customer service representative discussing CPNI with a customer, or of a bill or other document containing a customer's CPNI mistakenly being sent to the wrong address. These situations are more appropriately and effectively addressed by employee training and discipline procedures, and do not require the expenditure of carrier reporting or government investigative resources.

Likewise, conduct or security weaknesses that theoretically or potentially could have led to exposure of CPNI (but where there is no evidence that they actually did) are matters for carrier corrective actions and employee training, but do not require the expenditure of carrier reporting or government investigative resources.

WTA agrees with CTIA that expansion of the definition of "breach" to include accidental, inadvertent, and potential incidents would "result in overreporting with no benefit to customers, and would ultimately harm rather than aid the FCC's [and FBI and USSS] security efforts."[1] The expanded definition includes no added consumer protection benefits, but is more likely to produce "notice fatigue" that can cause customers receiving frequent breach notices to overlook or respond inadequately to notices of significant breaches. And it would inundate the Commission, FBI and

[1] Comments of CTIA, WC Docket No. 22-21 (February 22, 2023) at p. 26

USSS with reports of minor, inadvertent incidents or even non-events that would divert limited investigative resources that are best focused upon the types of substantial, intentional data breaches that are most likely to cause significant harm.

Harm-Based Notification Trigger

Should the Commission, for any reason, decide to include accidental, inadvertent or potential incidents in its definition of "breach," it should also adopt a harm-based notification trigger with respect to such incidents. In fact, further consideration of the matter has convinced WTA that a harm-based notification trigger should be employed to determine whether a service provider is required to report any CPNI data breach whether intentional, accidental, inadvertent or potential. A requirement of substantial harm allows government agencies to focus their time and energy on incidents where investigation and mitigation will be most useful, and to avoid low-impact situations that will drain government resources.

WTA agrees with NCTA that the requisite "harm" must be defined as actual and concrete harm, such as physical harm, identity theft, theft of service, and financial harm.[2] In contrast, "harm" should not include speculative, amorphous and potentially subjective elements such as potential damage to reputation or emotional harm.[3] A clear and specific definition of "harm" will give covered service providers a standard that can be consistently and objectively applied while ensuring that the Commission, FBI, USSS and customers receive timely reports of substantial and

[2] Whereas the existence of some amount of financial harm should be included as part of a harm-based notification trigger, it is not possible to determine or predict the actual or likely amount of such financial harm with any degree of accuracy during the brief and chaotic period immediately following discovery of a data breach. Rather, it generally takes carriers several weeks or months after discovery of a breach to ascertain the direct and indirect damages and costs of investigation and remediation incurred by both the carriers themselves and by their customers.

[3] Comments of NCTA–The Internet & Television Association, WC Docket No. 22-21 (February 22, 2023) at pp. 5-6. See also, Comments of Competitive Carriers Association, WC Docket No. 22-21 (February 22, 2023) at p. 5 ("NCTA Comments").

harmful CPNI breaches without being inundated by numerous reports of harmless or relatively harmless incidents.

Threshold Trigger

WTA reiterates that the Commission should set a threshold for the number of customers affected by a CPNI data breach before such breach is required to be reported to the Commission, FBI and USSS. WTA has proposed a threshold of five thousand (5,000) affected customers.[4] Verizon indicated that a threshold reporting trigger for large carriers like itself should be considerably more than 1,000 affected customers.[5] The critical factor here is not the difference between large and small service providers, but rather the balance between the need for government assistance to investigate and recover from significant database breaches vis-a-vis the need to prevent government resources from being bogged down by the investigation of so many small breach incidents that they are unable to respond as fully and rapidly as needed to major incidents.

WTA reiterates that a threshold trigger does not mean that carriers may relax their cybersecurity procedures, or that they do not need to respond fully and promptly to data breaches and to notify affected customers. All carriers have legal responsibilities to protect the confidential data of their customers, and to comply with the conditions of their cybersecurity insurance policies. All that a reporting threshold means is that carriers do not have to report certain CPNI data breaches affecting relatively small numbers of customers to the Commission, FBI and USSS in order to avoid flooding them with numerous reports of small incidents that can delay or impair their responses to larger incidents.

[4] A 5,000-customer threshold constitutes 0.00515 percent (a very small fraction of one percent) of the nation's 97.6 million fixed retail voice telephone service subscriptions. *2022 Communications Marketplace Report,* GN Docket No. 22-203, FCC 22-103, released December 30, 2022.
[5] Comments of Verizon, WC Docket No. 22-21 (February 22, 2023) at pp. 11-12.

Social Security Numbers and Financial Information

WTA agrees with NCTA[6] and the Information Technology Industry Council[7] that Section 222 of the Communications Act (and particularly subsections 222(c) and 222(h)(1)) gives the Commission jurisdiction only over data breaches involving CPNI and does not encompass data breaches involving non-CPNI data such as social security numbers and personal financial information.[8] This latter information is subject to the jurisdiction of other federal agencies such as the Federal Trade Commission and of various state statutes and agencies.

WTA would love to see a single set of common data breach reporting requirements for all federal and state agencies. However, unless and until that day comes, the Commission's reporting requirements should be limited to CPNI data breaches and should not be extended into additional data categories where they may come into conflict with the reporting requirements of other federal and state agencies.

Flexible Customer Notifications

WTA agrees with John Staurulakis, LLC,[9] USTelecom[10] and NTCA[11] that the requirements for notification of customers regarding data breaches should be flexible. WTA recognizes the importance of notifying customers as soon as practicable, but notes that identifying and notifying the particular customers who are potentially impacted by a breach is much more complicated and

[6] NCTA Comments at pp. 12-15.
[7] Comments of The Information Technology Industry Council, WC Docket No. 22-21 (February 22, 2023) at pp. 4-5.
[8] WTA notes that the proposals in the Comments on Notice of Proposed Rulemaking by the Electronic Privacy Information Center ("EPIC"), WC Docket No. 22-21 (February 22, 2023) for very expansive Commission jurisdiction over data breaches are based upon data security breaches and impacts that go far beyond CPNI and the Commission's Section 222 jurisdiction.
[9] Comments of John Staurulakis, LLC, WC Docket No. 22-21 (February 22, 2023) at pp. 6-7.
[10] Comments of USTelecom – The Broadband Association, WC Docket No. 22-21 (February 22, 2023) at pp. 6-8
[11] Comments of NTCA – The Rural Broadband Association, WC Docket No. 22-21 (February 22, 2023) at pp. 8-9

difficult than notifying government agencies that a breach has occurred. It generally takes at least several days for breached databases to be inspected and restored, and may take weeks after that to complete the forensic analyses necessary to identify affected customers. WTA notes: (a) that the *NPRM* contemplates (at paragraph 37) customer notification delays of up to thirty (30) days if requested by law enforcement; (b) that various states appear to have outside limits of 30, 45 or 60 days for customer notifications after a breach (*NPRM*, paragraph 34); and (c) that the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") rules for notifying individual patients "without unreasonable delay" of breaches entailing access to their sensitive personal medical data employ a maximum notification deadline of sixty (60) days after discovery of the breach. WTA supports a policy of customer notification "without unreasonable delay" but with a flexible time period that allows up to sixty (60) days after discovery of a breach for customers to be notified.

Conclusion

WTA continues to believe that the most effective and efficient reform of the Commission's CPNI data breach reporting requirements would entail the coordination thereof with those of other federal and state agencies so that the growing number of cybersecurity reporting requirements and timeframes are consistent with each other to the maximum feasible extent. On specific issues, WTA: (a) supports the continued limitation of the definition of "breach" to intentional actions; (b) supports the use of a harm-based trigger for data breach reporting obligations to limit over-reporting and preserve investigative and reporting resources; (c) supports a threshold trigger of 5,000 affected customers to further limit over-reporting and preserve investigative and reporting

resources; (d) opposes extension of reporting requirements beyond the statutory CPNI limits of Section 222 of the Communications Act; and (e) supports flexibility for customer notifications.

Respectfully submitted,
WTA – ADVOCATES FOR RURAL BROADBAND

/s/ Derrick B. Owens
Senior Vice President of Government and Industry Affairs

/s/ Gerard J. Duffy
Regulatory Counsel

400 Seventh Street NW, Suite 406
Washington, DC 20004
Phone: (202) 548-0202

Dated: March 24, 2023