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 NTCA–THE RURAL BROADBAND ASSOCIATION

NTCA–The Rural Broadband Association ("NTCA")[1] hereby submits these reply comments in response to the Notice of Proposed Rulemaking ("Notice") released by the Federal Communications Commission ("Commission") in the above-captioned proceeding.[2] The Commission seeks comment in the Notice on methods of updating the rules adopted in 2007 governing breaches of telecommunications carriers' customer proprietary network information ("CPNI"). In particular, the Notice seeks comment on appropriate and effective methods of updating CPNI breach notices to law enforcement, the Commission and customers.

Commenters, including NTCA, universally supported the Commission's goal of ensuring law enforcement and customers receive timely notice of CPNI breaches. Nearly all commenters, however, urged the Commission to ensure that breach notices are meaningful to law

[1] NTCA–The Rural Broadband Association represents approximately 850 independent, community-based companies and cooperatives that provide advanced communications services in rural America and more than 400 other firms that support or are themselves engaged in the provision of such services.

[2] *Data Breach Reporting Requirements,* Notice of Proposed Rulemaking, WC Docket No. 22-21, FCC 22-102 (rel. Jan. 6, 2023).

enforcement, the Commission, and customers and do not conflict with, or duplicate, existing state breach reporting requirements. Commenters further recommended that the Commission's rules clearly define the instances in which carriers must report breaches and allow carriers to make a reasonable determination that a breach occurred prior to the timeline for reporting a breach commences. Finally, NTCA and other commenters urged the Commission to avoid prescribing the contents of customer breach notices due to the burden additional reporting requirements would impose on carriers and the risk that consumers would be confused by receiving multiple notices for the same breach.

I. THE RECORD OVERWHELMINGLY SUPPORTS THE USE OF A CLEARLY DEFINED TANGIBLE HARM STANDARD FOR BREACH NOTIFICATIONS.

Commenters largely supported the Commission's proposal to adopt a harm-based trigger for notifying law enforcement and customers of a breach; however, commenters simultaneously urged the Commission to establish a clearly defined, tangible harm to avoid confusion and over reporting. Specifically, joining NTCA in recommending the Commission require carriers to report CPNI breaches only where the carrier believes there is a reasonable likelihood of financial harm, ACA Connects, JSI, Verizon, NCTA and WISPA all recommended the Commission define harm for purposes of CPNI breach notifications as circumstances that carriers reasonably believe would result in financial harm to the customers whose information was accessed.[3] Multiple commenters also encouraged the Commission to define harm for these purposes as either financial harm or identity theft, both of which offer clear standards for carriers while

[3] Comments of ACA Connects, WC Docket No. 22-21 (Feb. 23, 2023) at p. 7 ("ACA Connects Comments"); Comments of NTCA, WC Docket No. 22-21 (Feb. 23, 2023) at p. 5 ("NTCA Comments"); Comments of JSI, WC Docket No. 22-21 (Feb. 23, 2023) at pp. 3-4 ("JSI Comments"); Comments of Verizon, WC Docket No. 21-21 (Feb. 23, 2023) at p. 10; Comments of NCTA, WC Docket No. 22-21 (Feb. 23, 2023) at p. 1 ("NCTA Comments"); Comments of WISPA, WC Docket No. 22-21(Feb. 23, 2023) at p. 5 ("WISPA Comments").

simultaneously allowing the Commission, law enforcement and customers to act swiftly on preventing further access to and use of customers' CPNI.

Commenters emphasized that the harm must be clearly defined as something tangible, to avoid confusion, inconsistency and/or over reporting. Even the Electronic Privacy Information Center ("EPIC"), while arguing against the use of a harm-based trigger, did so out of concern that a harm threshold "can result in legal ambiguity," "underreporting," and "delayed reporting."[4] Furthermore, as the Competitive Carriers Association commented, requiring carriers to determine whether subjective harms are reasonably likely "could itself raise privacy concerns" in addition to "creating confusion and inconsistency."[5]

Thus, based on the record, if the Commission concludes that revising the current definition of breach to eliminate the "intentional" requirement would benefit consumers and carriers, the Commission must use caution to avoid adopting a new definition that creates more burdens for consumers and carriers due to the ambiguity of when the standard is met.

II. THE RECORD SUPPORTS MAINTAINING THE TIME PERIOD DURING WHICH PROVIDERS CAN MAKE A REASONABLE DETERMINATION AS TO WHETHER A BREACH OCCURRED.

In response to the Commission's request for comment on the appropriate timeframe for carriers to report breaches to the Commission and law enforcement, commenters overwhelmingly recommended maintaining the current requirement that the timeframe does not begin until carriers have made a reasonable determination that a breach occurred. ACA Connects and Sorenson Communications joined NTCA in encouraging the Commission to maintain the current

[4] EPIC Comments, WC Docket No. 22-21 (Feb. 23, 203) at p. 8.

[5] Comments of Competitive Carriers Ass'n, WC Docket No. 22-21 (Feb. 23. 2032) at p. 5 ("CCA Comments").

requirement that carriers report a CPNI breach to law enforcement (and the Commission if the Commission adopts the Notice's proposal to require carriers to report breaches to the Commission as well) within seven business days following a carrier's reasonable determination that a breach has occurred.[6] As Sorenson Communications noted, this timeframe "allows providers a reasonable opportunity to investigate potential incidents, determine whether a breach is reasonably likely to have occurred, and report it to law enforcement if necessary."[7]

While several commenters encouraged the Commission to instead require carriers to report breaches to law enforcement "as soon as practicable" in lieu of the existing seven business days requirement, this approach is problematic.[8] For one thing, neither the commenters who supported reporting breaches "as soon as practicable" nor the Commission offered any basis for changing the rule or any demonstration that the existing seven business day timeline is somehow inadequate. Even worse, requiring breaches to be reported "as soon as practicable" can be interpreted differently by different carriers or even by law enforcement and the Commission, thereby placing carriers at risk of inadvertently violating the Commission's rules if they construe "as soon as practicable" differently than the Commission. By contrast, the current timeline provides certainty for carriers while simultaneously assuring law enforcement and customers that they will receive prompt notice of a CPNI breach. Carriers who are able to report CPNI breaches earlier than seven

[6] *See* ACA Connects Comments at p. 10; Comments of Sorenson Communications, LLC, WC Docket No. 22-21 (Feb. 23, 2023) at p. 5 ("Sorenson Comments"), and NTCA Comments at p. 7.

[7] Sorenson Comments at p. 5.

[8] *See* CCA Comments at p. 6, Comments of USTelecom, WC Docket No. 22-21 (Feb. 23, 2023) ("USTelecom Comments"); Comments of CTIA, WC Docket No. 22-21 (Feb. 23, 2023) at p. 34 ("CTIA Comments"); Comments of ITI, WC Docket No. 22-21 (Feb. 23, 2023) at p. 3; and NCTA Comments at p. 9.

business days after making a reasonable determination that a breach has occurred can do so without a need to modify the Commission's rules.

NTCA does not object to commenters that supported the Commission's proposal to require carriers to notify customers of CPNI breaches without unreasonable delay following notification to law enforcement;[9] however, when evaluating whether a delay is "unreasonable," the Commission should account for the practicality that identifying affected customers – especially if the data has been encrypted or selectively exfiltrated – followed by mailing notices to affected customers at their address of record via the U.S. Postal Service can take several weeks. Additionally, as the Commission noted, law enforcement can continue to direct carriers to temporarily refrain from notifying customers on a case-by-case basis.[10]

III. THE RECORD DOES NOT SUPPORT PRESCRIBING THE CONTENT OF CUSTOMER BREACH NOTIFICATIONS, AS THIS WOULD IMPOSE AN UNNECESSARY BURDEN ON CARRIERS AND LEAD TO CUSTOMER CONFUSION.

The Commission's current rules specify when, and to whom, breach notifications must be made, but do not address the content of customer notifications. The Commission sought comment in the Notice on whether to require customer breach notifications to include specific information. Nearly every commenter urged the Commission not to prescribe the content of these notifications due to the risk that the prescribed content could differ from state requirements and would restrict carriers' ability to adapt the content of notices to the specific circumstances of a breach.[11]

[9] *See* NTCA Comments at pp. 6-7; USTelecom Comments at pp. 6-7; NCTA Comments at p. 9.

[10] Notice at ¶ 31.

[11] Notice at ¶ 38.

Commenters also noted that the Notice did not offer any indication that the Commission's current rules are somehow insufficient for customers or carriers and, as a result, need to be changed.

Commenters additionally largely recommended the Commission avoid prescribing the content of customer notifications. CTIA, for instance, noted that "impacted customers are already receiving relevant information in a timely matter, including through notices that must be given to individual consumers under state law, as well as through other channels. … Imposing additional form and manner requirements would merely add complexity and confusion…."[12] Many carriers, including small ones, provide service in multiple states and therefore must already adhere to multiple states' laws regarding breach notice requirements. Adding yet another set of requirements - that has the potential to differ from even one of those state requirements - creates a significant burden on these carriers by requiring staff time to be devoted to preparing and sending out a second, possibly conflicting, notice to all affected customers at a time when the staff is needed to address the breach and maintain operations. Instead, the Commission can accomplish the same objective by instructing carriers to provide customer notifications in accordance with the requirements of the state in which they provide service to customers whose information was accessed.

The Commission itself recognized in the Notice that "[a]ll 50 states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands have laws requiring private or governmental entities to notify individuals of breaches involving their personal information."[13] Accordingly,

[12] CTIA Comments at pp. 31-33.

[13] *See* Notice at ¶ 39. *See also* "Security Breach Notification Laws," National Conference of State Legislatures (Jan. 17, 2022), https://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notificationlaws.aspx (last visited March 20, 2023).

dictating the contents of customer data breach notifications is unnecessary and risks not only subjecting carriers to rules that differ from state requirements but also customer confusion. The current rules correctly leave carriers with discretion to tailor the language and method of notification based on the nature of the data breach and varying circumstances, including any state data breach notification requirements. As USTelecom noted, the Notice "does not suggest the Commission's longstanding flexible approach to the content and form of CPNI breach notifications has failed to serve consumers…."[14]

EPIC and WISPA supported the Commission's proposal to impose minimum content requirements.[15] WISPA, however, recommended the prescribed content be "similar to content requirements in state data breach laws."[16] EPIC, meanwhile, supported the content requirements identified in the Notice without any suggestion that states' content requirements are lacking important information.[17] Accordingly, if states' content requirements are sufficient for providing customers with necessary information, there should be no need for the Commission to impose the same, much less different, requirements.

NTCA therefore encourages the Commission to carefully examine whether adopting minimum content requirements for customer breach notifications would achieve the intended result or would instead impose an unnecessary burden on carriers and create customer confusion. In the event the Commission concludes that providing suggested language would be beneficial to

[14] USTelecom Comments at pp. 8-9.

[15] EPIC Comments at p. 8.

[16] WISPA Comments at p. 10.

[17] EPIC Comments at p. 8.

carriers and customers, NTCA urges the Commission to establish clear guidance regarding the content of such notices.[18]

IV. CONCLUSION

Commenters universally supported the Commission's goal of assisting carriers and consumers protect CPNI. When evaluating whether changes are necessary to achieve this objective, however, NTCA encourages the Commission to first identify where, if at all, the existing rules fall short; to avoid uncertainty and confusion by providing clear definitions of carriers' requirements; and avoid imposing unnecessary burdens on carriers or confusing customers through duplicative reporting requirements.

Respectfully submitted,

By: */s/ Michael Romano*
Michael Romano
Jill Canfield
Tamber Ray
Blain Tesfaye

4121 Wilson Boulevard, Suite 1000
Arlington, VA 22203

(703) 351-2000

[18] *See, e.g.*, NTCA Comments at pp. 8-9.