**Before the**
**Federal Communications Commission**
**Washington, D.C. 20554**

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

**COMMENTS**
**OF**
**NTCA–THE RURAL BROADBAND ASSOCIATION**

NTCA–The Rural Broadband Association ("NTCA")[1] hereby submits these 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"). NTCA supports the Commission's goal of assisting carriers with respect to guarding against breaches of customers' personal information. When considering modifications to the Commission's rules to accomplish this objective, however, NTCA encourages the Commission to forego requiring breach notifications to customers, the Commission and law enforcement (i.e., the Secret Service and the FBI) in instances where carriers have made a reasonable determination

[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).

that no financial harm to customers is reasonably likely to occur. NTCA further asks the Commission to limit carriers' obligation to provide reports of breaches to instances where the carrier reasonably believes at least 1,000 customers' CPNI was accessed used or disclosed. Finally, NTCA recommends retention of the current timeline for reporting breaches to the Commission and law enforcement and that the agency avoid prescribing the content of customer breach notices.

## I. INTRODUCTION

The Telecommunications Act of 1996[3] introduced comprehensive regulations governing the protection of CPNI. These standards are set forth in Section 222 of the Act and promulgated in 47 CFR sec. 64.2001 *et seq.* Specifically, CPNI covers "(A) Information that relates to the quantity, technical configuration, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and (B) information contained in the bills pertaining to telephone exchange service or telephone toll services received by a customer of a carrier."[4] Carriers are required to certify annually that they adhere to these requirements, including a description of the processes and procedures they employ to ensure compliance. Notably, CPNI requirements address only telecommunications services; they do not address broadband internet access services. Moreover, the Commission has ruled explicitly that it

[3] Telecommunications Act of 1996, Pub. L. No. 104-104, 110 Stat. 56 (1996) (1996 Act). The 1996 Act amended the Communications Act of 1934 and is codified at 47 U.S.C. § 151 *et seq.,*and is hereafter referred to in these comments as "the Act."

[4] 47 U.S.C. § 222(h)(1).

will not preempt state rules governing CPNI to the extent those rules do not conflict with Federal regulations.[5]

The Commission now seeks to expand the applicability of CPNI to broader circumstances and conditions while at the same time refining notification requirements with respect to certain instances of access to CPNI. In particular, the Commission proposes a number of modifications to the current rules governing the definition of a breach, the timing for notifying the Commission, the Secret Service and the FBI of a breach, and when and how customers are to be notified of a breach.[6]

Any changes to the rules that define a breach or trigger notifications related to these must be structured in a manner that provides for meaningful reports that will assist the Commission, law enforcement, other carriers and customers in guarding against similar events. CPNI reporting rules also must be aligned with existing federal and state laws governing breach of customers' information to the greatest degree possible, including providing reasonable flexibility for the contents of customer breach notifications in order to allow carriers to align any notices with other state and federal laws.

## II. ADOPTING A WELL-DEFINED REASONABLE LIKELIHOOD OF FINANCIAL HARM STANDARD FOR ANY CPNI REPORTING REQUIREMENT WILL BEST ACCOMPLISH THE COMMISSION'S GOALS.

The Commission's current rules define breach as "when a person, without authorization or exceeding authorization, has intentionally gained access to, used, or disclosed CPNI."[7] The Commission proposes in the Notice to expand this definition to include "inadvertent access, use,

[5] *See 2007 CPNI Order*, 22 FCC Rcd at 6957-58, ¶ 60.
[6] Notice at ¶ 11.

[7] 47 CFR § 64.2011(c).

or disclosures of customer information."[8] The Commission concludes that this expanded definition is necessary due to the inability to know with certainty whether certain breaches were intentional – thereby leading to ambiguity and possible under reporting – as well as the possibility that inadvertent disclosures of CPNI could result in misuse of such information.

NTCA recognizes that determining intent for purposes of CPNI breaches,[9] as required under the Commission's current rules, can be difficult to ascertain and can exclude some breaches that have the potential to cause harm. NTCA also recognizes the importance of ensuring the Commission and customers are notified of breaches so they can take steps to prevent future breaches and guard against the information that may have been accessed during the breach being misused. Any changes to the definition of a breach, however, must be as precise as possible to avoid substituting one kind of ambiguity and uncertainty for another. Furthermore, simply removing the current "intentional" requirement so that the definition also encompasses inadvertent access, use or disclosure[10] could create significant burdens on carriers, the Commission and law enforcement. In particular, such rules would impose substantial challenges on carriers to obtain notice from employees or contractors of every inadvertent access, use or disclosure of CPNI, while also requiring a substantial amount of time by carriers to review such incidents to determine if they rise to a level necessitating notification to the Commission, law enforcement and affected customers.

[8] Notice at ¶ 12.

[9] *Id*. at ¶ 13.

[10] *Id.* at ¶ 12.

Quite simply, the burden on carriers, the Commission and law enforcement if every inadvertent or accidental access to or use of CPNI was reported would be substantial. The Commission itself recognized that "the vast majority of state statutes" exclude good-faith acquisition of CPNI by an employee or agent of the company if such information is not used improperly or further disclosed.[11] Therefore, NTCA recommends the Commission forego requiring notification of CPNI breaches to the Commission, law enforcement or customers in instances where a carrier determines that no financial harm is reasonably likely to occur as a result of the breach.

Applying a harm-based trigger for data breach notifications would allow carriers, the Commission and law enforcement to focus on assisting customers in recovering from any damage that may have resulted from the breach. NTCA cautions, however, that to avoid confusion and unnecessary reports, the Commission must provide a clear, tangible and consistent definition of harm. Thus, emotional harm, for instance, should not qualify as a harm-based trigger due to the substantial difficulty of defining such harm and the likelihood that carriers would be unaware of whether emotional harm occurred prior to the deadline for reporting a breach. Instead, a data breach notification requirement should be limited to breaches in which a carrier has reasonably determined that financial harm may occur as a result of the breach.

NTCA further encourages the Commission to require carriers to submit breach reports to the Commission and law enforcement only in instances where a carrier determines that the breach has resulted in the access, use or disclosure of at least 1,000 customers' CPNI. This will allow the Commission and law enforcement to focus on instances where they can work together to help

[11] *Id*. at ¶ 13.

carriers guard against similar breaches and take action against the perpetrator of the breach. Requiring carriers to maintain records of any additional breaches that do not meet these definitions will place an unnecessary burden on carriers, which the Commission sought to avoid.[12]

## III. THE COMMISSION SHOULD RETAIN THE CURRENT TIMEFRAME FOR REPORTING BREACHES TO LAW ENFORCEMENT AND THE COMMISSION.

The Commission's rules currently require carriers to notify the FBI and Secret Service of CPNI breaches no later than seven business days after reasonable determination of the breach. Carriers must then wait at least seven business days following notice to the FBI and Secret Service before notifying customers of the breach, absent authorization to provide earlier customer notification. In the Notice, the Commission proposes to expand carriers' reporting requirement to include notification to the Commission, as well as the FBI and Secret Service, "as soon as practicable after discovery of a breach" and to require customer notification "without unreasonable delay" after notification to law enforcement.[13]

As an initial matter, NTCA does not oppose requiring carriers to report CPNI breaches to the Commission simultaneously with the Secret Service and FBI, provided carriers only need to submit one report and the report can be submitted using the link already provided on the Commission's website for reporting CPNI breaches.[14] NTCA also supports the Commission's

[12] *Id.* at ¶ 26 ("We seek comment on how we can minimize data breach reporting burdens for telecommunications carriers.").

[13] *Id*. at ¶¶ 28, 31.

[14] The Commission suggests in the Notice that CISA's Incident Reporting System could be used for this purpose, in lieu of a reporting portal on the Commission's website, to reduce the reporting burden on carriers. *See* Notice at ¶ 25. NTCA supports avoiding duplicative reporting requirements; however, while CISA currently has a voluntary cyber incident reporting form on its website, carriers should have the opportunity to offer feedback pursuant to the forthcoming CIRCIA rulemaking proceeding on the information to be provided in incident reports and how that information will be protected and shared with the Commission and law enforcement officials prior to the Commission directing carriers to use this method of reporting.

proposal to require notice to affected customers "without unreasonable delay" following notice to the Commission and law enforcement. NTCA recommends, however, that the Commission maintain the current "within seven business days following reasonable determination" timing for carriers to report any breach to the Commission and law enforcement.

The Commission does not offer any basis for modifying the reporting timeline – noting only the importance of providing the Commission with such information so that the Commission can "help address and mediate" any data security vulnerabilities.[15] Furthermore, carriers often require several days or more to conduct a forensic analysis of a breach, which is necessary to identify the cause, source, and potential impacts of such breach. Small carriers in particular will often need to hire an outside consultant to conduct this analysis, which will very likely add to the amount of time needed to complete the analysis. As a result, a forensic analysis will routinely require a week or more to complete. Therefore, absent some evidence that the current timeline is inadequate to accomplish the Commission's goals, carriers would benefit from the current defined seven-day timeframe rather than being at risk of interpreting "as soon as practicable" differently than the Commission. Carriers should be assured of a sufficient timeframe for completing a breach report that provides all of the information needed by the Commission and law enforcement to assist in mitigating customer harm and providing guidance to providers.

Adopting an undefined deadline for reporting data breaches could also be interpreted as earlier than the current CPNI breach reporting timeframe, which could result in carriers filing reports with the Commission that do not include the information the Commission and law

[15] *Id*. at ¶ 24.

enforcement officials need to be able to attempt to prevent further dissemination of the information accessed or to identify actions other carriers can take to minimize their risk of a similar breach.

## IV. THE CONTENT OF CUSTOMER BREACH NOTICES MUST BE FLEXIBLE.

The Commission's rules do not currently specify the information that carriers must include in notices to customers of CPNI breaches and the Commission specifically refrained from prescribing the content of customer notices when adopting the CPNI rules, instead leaving the content of such notices to carriers' discretion.[16] The current rules have withstood the test of time for nearly 15 years and the Commission does not now suggest that customer notices are somehow deficient. Thus, dictating the contents of customer data breach notices is unnecessary and risks subjecting carriers to disparate state and possibly even federal reporting requirements. 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.

Nevertheless, if the Commission concludes that offering guidance to carriers regarding the information to include in customer notices would be beneficial, NTCA encourages the Commission to address the following questions as part of that guidance:

1. If the date of the breach should be included, what date should a carrier use if the exact date is unknown?
2. If a description of the customer information that was used, disclosed, or accessed must be included, how would a carrier know how such information was used?

[16] *Id.* at ¶ 38.

3. If the notice must contain information about how to contact the Commission, the FTC, and any state regulatory agencies relevant to the customer and service, will there be/is there contact information at each of these agencies specifically for data breaches or should the carrier include the main agency contact information? Will the Commission provide a list of "relevant" state regulatory agencies or will carriers be expected to know the relevant agencies and their contact information?
4. Finally, if carriers should include "other steps customers should take to mitigate their risk based on the information exposed in the breach," would the Commission provide recommended steps carriers could include in the notice and would the steps need to be modified depending on the specifics of a particular breach?

These questions demonstrate the difficulty with mandating the contents of customer breach notices. Thus, while adopting a "one size fits all" approach to the content of customer notices is unnecessary and could conflict with other customer notice requirements, if the Commission concludes that providing suggested language would be beneficial to carriers and customers, NTCA recommends the Commission offer clear guidance regarding the suggested content of such notices.

## V. CONCLUSION

NTCA supports the Commission's goal of assisting carriers and consumers protect CPNI. When updating existing rules to achieve this objective, however, the Commission should modify only those rules that have been found to leave gaps in law enforcement's ability to act on breaches. The Commission must also avoid promulgating rules that create additional burdens and uncertainty on carriers by being poorly defined, that impose recordkeeping or notice requirements that do not assist carriers or customers recover or act on the breached data, and that risk conflicting with other state and federal laws.

Respectfully submitted,


By: */s/ Michael Romano*

Michael Romano
Tamber Ray
Josh Seidemann
Blain Tesfaye

4121 Wilson Boulevard, Suite 1000
Arlington, VA 22203

(703) 351-2000