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

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

COMMENTS
OF
WTA – ADVOCATES FOR RURAL BROADBAND

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

WTA notes that the Customer Proprietary Network Information ("CPNI") usage and security provisions adopted in Section 222 of the Telecommunications Act of 1996 and implemented in Subpart U of Part 64 of the Commission's Rules have morphed over the years from (a) initial limitations on the potential ability of monopoly local exchange carriers to use CPNI data to gain marketing advantages in competitive markets to (b) the current focus on cybersecurity measures and reporting to safeguard CPNI from unauthorized access, theft and abuse. WTA believes that the Commission should expand its review of the CPNI rules to reassess the post-1996 impacts of changing market conditions and technologies upon legacy CPNI marketing restrictions as well as to review and clarify its CPNI data breach reporting requirements.

WTA

WTA is a national trade association that represents more than 360 rural local telecommunications carriers ("RLECs") that provide voice, broadband and other services to some of the most rural, remote, rugged, sparsely populated, and expensive-to-serve areas of the United States. WTA members have long constructed and operated rural voice and broadband networks – very often as providers of last resort – in high-cost farming, ranching, mining, mountain, forest and desert areas, as well as on Native American reservations and other Tribal Lands.

Changed Conditions Merit Reassessment of CPNI Marketing Restrictions

Most WTA members offer the bundles of voice, broadband and/or video services wanted by many of their customers, but do not use the CPNI generated by their voice telecommunications services to design and market these bundles or to market any other non-telecommunications services. Those WTA members that may utilize CPNI from time to time in their marketing efforts follow the "opt-in" and "opt-out" procedures set forth in the Commission's Part 64 rules.

Section 222 of the Telecommunications Act of 1996 and the Commission's implementing CPNI rules were adopted at a time when there was considerable concern that the recently divested Baby Bells and other dominant large carriers would use the CPNI generated by their monopoly local exchange voice services to gain unfair competitive advantages in markets for long distance toll services and for various related and unrelated non-telecommunications services. However, twenty-seven years later, the once formidable wireline local exchange voice telecommunications service monopolies are long gone, having lost substantial market share to mobile wireless and Voice over Internet Protocol ("VoIP") services while the national telecommunications network has evolved from a voice-centric network to the current higher-and-higher-speed broadband

network. As a result, the CPNI generated by wireline local exchange voice telecommunications services no longer constitutes the substantial competitive marketing advantage that it did during the late 1990s when most of the current CPNI rules were adopted.

Moreover, the core business plans of major broadband service providers such as Google, Facebook, and Amazon employ the email, social media, web browsing and online purchasing activities of broadband users to construct individual customer profiles that are sold to advertisers or otherwise used directly and indirectly to market goods and services. These broadband customer profiling practices are far more extensive, and have much greater impacts upon privacy and competitive markets, than the potential CPNI marketing uses addressed and restricted in Section 224 and Part 64.

WTA does not know what, if anything, the Commission can do about current broadband profiling practices under existing statutes and regulatory classifications. However, it is grossly unfair that voice telecommunications carriers are subject to substantial restrictions on their use of CPNI for marketing purposes while large broadband edge service providers are free to employ a far more comprehensive and intrusive variety of CPNI-like usage data for marketing purposes without significant restriction. WTA suggests that a fair and reasonable approach would be for the Commission to reassess its rules limiting the use of CPNI for marketing purposes, with the goal of eliminating or modifying or forbearing from those that are no longer necessary or effective under current market conditions.

Modifications to Data Breach Reporting Requirements

WTA and its members are actively engaged in the implementation, monitoring and improvement of their cybersecurity safeguards in the face of frequently changing intrusion tactics. Among other measures, many WTA members are studying and adapting the National Institute of Standards and Technology ("NIST") cybersecurity frameworks and following the Cybersecurity and Infrastructure Agency's ("CISA's") implementation of the Cyber Incident Reporting for Critical Infrastructure Act of 2022 ("CIRCIA"). They must also deal with a variety of state privacy, consumer protection and cybersecurity legislation and regulations.

Method of Notification. Under Section 64.2011(b) of the Rules, WTA members and other telecommunications service providers must notify the Federal Bureau of Investigation ("FBI") and the United States Secret Service ("USSS") of covered breaches of CPNI data via a central reporting facility to which the Commission maintains a link. WTA has no objection to the Commission's proposed creation of a centralized portal for reporting CPNI data breaches to it as well as to the FBI and USSS. It makes good sense to have a single governmental point of contact for data breach reports, or at least as few as possible. It may be even more efficient to incorporate the Commission's data breach reporting portal into the CISA Incident Reporting System if that is practicable and minimizes duplicative reporting burdens for carriers.

Contents and Timeframe. WTA's primary concern is that the staffs of its members – and particularly the smaller staffs of its smaller members – not be overburdened and confused by a variety of differing reporting formats and timeframes for the same data breach incident. A company should not have to prepare and file three different reports with three separate federal or state agencies according to three varying deadlines, and then have to follow-up by sending one or more notices to customers in different formats and according to differing timetables. Such a

multiplicity of reporting requirements and schedules not only is inefficient and disruptive per se, but also is likely to prevent RLEC staffs from focusing their full attention upon the more critical tasks of data and operational recovery after a breach incident.

Most of the Commission's existing requirements regarding the contents of data breach notifications to federal law enforcement agencies are generally reasonable. It would appear that the following information should be standard for all data breach notices: (a) carrier contact information; (b) description of the data breach incident; (c) method or tactics of compromise; (d) date that breach was discovered and approximate date(s) that the breach took place, if different; (e) the types of data breached; and (f) the approximate number of customers affected.

However, WTA notes that "estimated financial loss" is impossible to determine or predict 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. And given that billing names and addresses (also known as subscriber list information) are not classified as CPNI, there does not appear to be any need to send the "addresses of affected customers" to multiple government databases as part of the initial incident notice before law enforcement and other agencies determine whether such addresses are relevant and required for their investigations.

WTA reiterates that the Commission's data breach reporting format is generally reasonable, but notes that the most effective reform that the Commission can accomplish is to coordinate its reporting format with other federal and state agencies so that the growing number of cybersecurity reporting requirements are consistent with each other to the greatest extent possible. WTA is well aware of potential jurisdictional and political issues, but hopes that this

area is ripe for coordination because the essential types of information needed to report a data breach to a government agency, and for the agency to begin investigating the breach, are virtually identical for every incident.

WTA believes that the timeframes for reporting data breaches to government authorities and to affected customers can and should also be standardized. The deadlines for initial reports to government agencies can be somewhere within a 5-to-10 business day range after discovery, depending upon the amount of information required to be included in the initial report. The most important factor from the efficiency and compliance standpoints is that the specified initial reporting deadlines be the same for all required federal and state government reports.

Likewise, the maximum time period for notifying affected customers should be standardized as much as possible across various agencies and jurisdictions. 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 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 safe harbor for customer notifications of sixty (60) days after discovery of a breach.

Threshold Trigger. WTA believes 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. A threshold of five thousand (5,000) affected customers would appear to constitute a reasonable 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.

A threshold does not mean that smaller 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 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.

Definition of "Breach." WTA believes that the existing Section 64.2011(e) definition of "breach" as an intentional action – that is, "when a person, without authorization or exceeding authorization, has intentionally gained access to, used, or disclosed CPNI" -- is more than sufficient to encompass any and all CPNI data breaches that should be reported to and investigated by the Commission, FBI and USSS. Government agencies have limited investigative resources, and these are best focused upon the data breaches that are most likely to cause significant harm –

that is, those where someone without appropriate authorization intentionally accesses protected CPNI data and/or intentionally uses or discloses such confidential CPNI data for non-permissible purposes.

WTA opposes the extension of the Commission's reporting requirements to accidental or inadvertent access, use or disclosure of CPNI. For WTA members, most such incidents are in the nature of an unauthorized employee or visitor inadvertently overhearing a customer service representative discussing CPNI with a customer, or of a document containing a customer's CPNI inadvertently 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.

Should the Commission, for any reason, decide to include accidental or inadvertent incidents in its definition of "breach," it should also adopt a harm-based notification trigger with respect to such incidents. Whereas intentional access to, or use or disclosure of, CPNI can reasonably be assumed to involve harm, many accidental or inadvertent incidents are not likely to result in any harm or damage. Hence, the Commission should not require carriers to report an accidental or inadvertent incident involving access, use or disclosure of CPNI if such carriers have a reasonable basis for believing that no harm is likely to occur to them or to their customers as a result of the incident.

Conclusion

WTA encourages the Commission to expand its review of the CPNI rules to reassess the post-1996 impacts of changing market conditions and technologies upon the initial CPNI marketing restrictions as well as to review and clarify its CPNI data breach reporting requirements.

In the latter area, the most effective and efficient reform would entail the coordination of the Commission's required reporting notifications and deadlines 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. While WTA supports a common Commission-FBI-USSS portal and a reporting threshold of at least 5,000 affected customers, it opposes expansion of the definition of reportable breaches beyond those involving intentional unauthorized access, use or disclosure.

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: February 22, 2023