Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

Information Collection Being Reviewed by the Federal Communications Commission	**)** **)** **)**	**OMB 3060-XXXX**
Protecting the Privacy of Customers of Broadband and Other Telecommunications Providers	**)** **)** **)**	**Docket No. 16-106**

COMMENTS OF

NTCA–THE RURAL BROADBAND ASSOCIATION

I. INTRODUCTION

NTCA–The Rural Broadband Association (NTCA)[1] hereby submits these comments in the response to the above-captioned Notice and Request for Comments ("Notice") published in the Federal Register on January 11, 2017.[2]

In October 2016, the Federal Communications Commission (Commission) adopted updated rules to address the obligations of broadband Internet access service (BIAS) providers under Section 222 of the Communications Act of 1934, as amended.[3] Among other obligations, the new rules require BIAS providers, to (1) notify customers, the Commission, the Federal Bureau of Investigation, and the Secret Service under certain circumstances when customer

[1] NTCA represents more than 800 independent, community-based telecommunications companies. All NTCA members are full service local exchange carriers and broadband providers, and many of its members provide wireless, cable, satellite, and long distance and other competitive services to their communities.

[2] 82 Fed. Reg. 3313 (Jan. 11, 2017).

[3] *See, Protecting the Privacy of Customers of Broadband and Other Telecommunications Services: Report and Order,* Docket No. 16-106, FCC 16-148 (2016).

proprietary information is breached, and (2) maintain records of breaches and breach notifications. NTCA submits that although these requirements are described as "on occasion reporting requirements" and "one-time reporting requirement,"[4] the rules in fact threaten potentially frequent and expansive scope of applicability. As described below, the information collection as envisioned by the rules is not necessary for the proper performance of the functions of the Commission, and should therefore not be approved by the Office of Management and Budget (OMB).

II. DISCUSSION

The Commission explains that data breach notification rules are intended to encourage providers to "adopt strong data security practices."[5] And, yet, the Commission states "[a]t the same time, unnecessary notification can cause notice fatigue, erosion of consumer confidence in the communications they receive from their provider, and inflated compliance costs."[6] These concerns attend the final rules that were adopted in the instant proceeding: they set the stage for unnecessary notifications; will cause notice fatigue; and ultimately diminish customer confidence in the usefulness of communications received from BIAS providers. Section 64.2006 of the Commission rules addresses date breach notification obligations. These requirements are slated to become effective on the later of June 2, 2017, or Paperwork Reduction Act (PRA) approval. These rules will supersede existing Section 64.2011.

[4] 82 Fed. Reg. 3313 (Jan. 11, 2017).

[5] Order at para. 261.

[6] *Id.*

The new requirements address notifications that BIAS and other telecommunications providers must provide to customers, the Commission, and Federal law enforcement agencies. The rules also address recordkeeping requirements of the providers.

Specifically, the rules require telecommunications carriers (including BIAS providers) to notify affected customers no later than 30 calendar days after the carrier reasonably determines that a breach has occurred, unless the carrier can reasonably determine that no harm to customers is reasonably likely to occur as a result of the breach. The provider is required to send written notification to both current and former customers, and to undertake a reasonable investigation to determine the last ascertainable postal address where necessary. Carriers are also required to notify the Commission of breaches. For breaches affecting 5,000 or more customers, notification must be provided within seven days after the provider reasonably determines that a breach has occurred; for breaches affecting fewer than 5,000 customers, such notification must be provided within 30 calendar days. Federal law enforcement must be notified for breaches that affect 5,000 or more customers.

Several factors weigh against a determination that these requirements pass PRA muster. They include: the scope of information covered by the rule; the definition of "customer;" the definition of "breach;" the definition of "harm," and; the phenomenon characterized by the Commission as "notice fatigue." When combined, they undermine the supposed effectiveness of the rules to further Commission policy.

In the first instance, the universe of persons protected by the rules expanded when the Commission ruled that "customer" is not only a current or former subscriber of the telecommunications service, but also an applicant for a telecommunications service.[7] The

[7] 47 C.F.R. 64.2002.

Commission defines "breach of security" as "any instance in which a person, without authorization or exceeding authorization, has gained access to, used, or disclosed customer proprietary information."[8] "Customer proprietary information" includes not only customer proprietary network information (CPNI), but also "personally identifiable information" (PII). The Commission did not provide an exhaustive list of information that would be defined as PII. Rather, the Commission offered illustrative, non-exhaustive examples of information that it determined would be linked or reasonably linked to an individual or device.[9] These data may include a user's physical address, email address, telephone number, and name.[10]

At this stage of the discussion, it is useful to assess the requirements and to extract that under the current rules, a telecommunications provider could be subject to the breach notification rules if an employee who generally does not have access to consumer records data inadvertently gains access to the name, address, and telephone number of an applicant for service.

To be sure, the notification requirements are triggered by the telecommunications carrier's determination that the breach reasonably likely to cause harm. However, the deadline for notification is grounded in the *breach itself,* rather than the carrier's determination of whether harm to the customer might occur. Accordingly, it is possible that there are instances in which it takes a telecommunications carrier more than seven days after the discovery of breach to determine whether harm is "reasonably likely to occur as a result of the breach,"[11] yet the carrier would be required to notify the Commission and/or Federal law enforcement in order to meet the seven-day deadline requirement. This could either leave providers with a severely truncated

[8] 47 C.F.R. 64.2002.

[9] Order at para. 89.

[10] Order at para. 93.

[11] *See,* 47 C.F.R. 64.2006(b), (c).

period in which to provide notice, or *de facto* place them past the deadline and out of compliance. If it takes a carrier longer than seven days to determine whether a breach was harmful, carriers might either (a) not notify consumers until past the deadline, or (b) notify customers unnecessarily or without sufficient information.

Accordingly, there arises the possibility of many situations in which a breach affecting 5,000 or more customers is discovered and although it is determined ultimately that no harm would likely occur as a result of the breach, carriers would be required to undertake notification actions in order to meet a short-deadline that is unrelated to the finding that triggers the underlying requirement. At the very least, OMB approval of this rule should be withheld until the notification deadline is linked to the timing of the finding of facts that trigger the notification requirement.

The rules also suffer infirmity because they are unnecessarily expansive. In addition to the vast scope of information that could trigger the notification requirement, the harm-based standard encompasses such an unduly broad range of impacts. Together, these undermine the likelihood that the rules can be implemented in a cogent and rational manner, thereby diminishing the likelihood that their effectiveness will further the purposes for which they are intended. Although the notification requirement is triggered by a harm-based standard, "harm" is defined by the Commission to include financial, physical, and emotional harm.[12] It is difficult to propose that a telecommunications provider would be positioned to render judgment on whether the release of various data would cause emotional harm, which itself is depends upon the individual characteristics of each customer. Similarly, whether a breach causes "reputational damage, personal embarrassment, or loss of control over the exposure of intimate personal

[12] Order at para. 266.

details"[13] is a standard whose evaluation in many instances would reach beyond reasonable evaluation where non-sensitive data has been breached. The Commission acknowledged the difference between sensitive and non-sensitive data when it ordered a "rebuttable presumption that any breach involving sensitive customer PI poses a reasonable likelihood of customer harm and would therefore require . . . notification."[14] Without waiving any arguments or positions relating to the appropriateness of such a "rebuttable presumption," NTCA submits that as a baseline matter, a breach of non-sensitive data should not trigger a requirement to assess the potential emotional, reputational, or physical welfare of a customer, and should therefore not be included within the breach notification requirement. In order to ensure proper performance of the functions of the Commission, the triggering information, at most, should be limited to sensitive information – names in combination with other elements of CPNI or PI, but not information that is analogous to SLI.

III. CONCLUSION

In sum, as written, the rules threaten to compel providers to issue breach notifications in instances in which either they are either (a) legally unnecessary or (b) of dubious value from the consumer perspective. Both outcomes will risk the effect of "notice fatigue," an issue noticed by the Commission, and ultimately condition users to ignore notifications after series of effectively "false alarms." Without waiving positions or arguments that NTCA might set before the Commission regarding pending petitions for reconsideration or other litigation, NTCA submits that the rules cannot be adjudged to further the proper performance of Commission functions in their current state. The rules contemplate an overly broad set of information for which

[13] Order at para. 267.

[14] *Id.*

notification might be required; an overly broad population to which notice must be provided; potentially require providers to provide notices before the fact-based trigger for the requirement can be ascertained; and lack a reasonable approach that would link tangible harm to injury in fact.

For these reasons, NTCA recommends the OMB to decline approval of the rules.

Respectfully submitted,

By:
/s/ Joshua Seidemann
Joshua Seidemann
Vice President of Policy
4121 Wilson Boulevard, Suite 1000
Arlington, VA 22203
jseidemann@ntca@ntca.org
703-351-2000 (Tel)

March 13, 2017