**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**
**USTELECOM – THE BROADBAND ASSOCIATION**

USTelecom – The Broadband Association ("USTelecom") submits these reply comments in response to the Federal Communications Commission's ("Commission" or "FCC") Notice of Proposed Rulemaking ("NPRM") seeking to update the Commission's rules regarding reporting breaches of customer proprietary network information ("CPNI").[1] The record overwhelmingly demonstrates the importance of ensuring that the Commission's CPNI breach reporting requirements are practical and flexible to best protect customers of telecommunications service.

## I. THE RECORD CONFIRMS THAT A HARM-BASED TRIGGER BEST BALANCES NOTIFICATION WITH THE RISK OF OVER-NOTIFICATION

The record reflects near unanimous support for adopting a harm-based trigger.[2] Consistent with USTelecom's initial comments, commenters explain that a harm-based trigger

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

[2] *See* Comments of USTelecom – The Broadband Association, WC Docket No. 22-21, at 3-6 (filed Feb. 22, 2023) ("USTelecom"); Comments of ACA Connects, WC Docket No. 22-21, at 3 (filed Feb. 22, 2023) ("ACA"); Comments of Blooston Rural Carriers, WC Docket No. 22-21, at 2 (filed Feb. 22, 2023) ("Blooston"); Comments of Competitive Carriers Association, WC Docket No. 22-21, at 5 (filed Feb. 22, 2023) ("CCA"); Comments of CrowdStrike, WC Docket No. 22-21, at 3 (filed Feb. 22, 2023) ("CrowdStrike"); Comments of CTIA, WC Docket No. 22-21, at 21-22 (filed Feb. 22, 2023) ("CTIA"); Comments of Hamilton Relay, Inc., WC Docket No. 22-21, at 6 (filed Feb. 22, 2023) ("Hamilton"); Comments of Information Technology Industry Council, WC Docket No. 22-21, at 3 (filed Feb. 22, 2023) ("ITI"); Comments of NCTA – The Internet & Television Association, WC Docket No. 22-21, at 4 (filed Feb. 22, 2023) ("NCTA"); Comments of NTCA – The Rural Broadband Association, WC Docket No. 22-21, at 5 (filed Feb. 22, 2023) ("NTCA"); Comments of Verizon, WC Docket No. 22-21, at 10 (filed Feb. 22, 2023) ("Verizon"); Comments of WISPA – Broadband Without Boundaries, WC Docket No. 22-21,

reduces the risks of over-notification and notice fatigue.[3] WISPA, for instance, notes that a harm-based trigger "benefit[s] consumers by avoiding confusion and notice fatigue with respect to breaches unlikely to cause harm…."[4] Likewise, Verizon offers that a harm-based trigger "prevent[s] customers from spending unnecessary time and money to protect their information based on a harmless breach."[5] Blooston adds that "requiring disclosure when there is no harm may unnecessarily confuse and alarm consumers and lead to 'notice fatigue.'"[6] Thus, a harm-based trigger "aligns the circumstances in which customers receive notice with the circumstances in which they should take action to protect themselves."[7]

Similarly, numerous commenters are aligned in pushing back on the Commission's proposal to expand its breach definition to include inadvertent breaches of CPNI.[8] Several note that expanding the definition creates a risk of over-reporting to the detriment of consumers.[9] To the extent the Commission expands the definition, commenters emphasize that the Commission

---

at 4-5 (filed Feb. 22, 2023) ("WISPA"); Comments of WTA – Advocates for Rural Broadband, at 8 (filed Feb. 22, 2023) ("WTA").

[3] *See, e.g.*, USTelecom at 3-6; ACA at 7; Blooston at 2; CCA at 6; CTIA at 22; Hamilton at 6; ITI at 3; Comments of John Staurulakis, LLC, WC Docket No. 22-21, at 4 (filed Feb. 22, 2023) ("JSI"); NCTA at 5; Comments of Sorenson Communications, LLC, WC Docket No. 22-21, at 4 (filed Feb. 22, 2023); Verizon at 10-11; WISPA at 5.

[4] WISPA at 4-5.

[5] Verizon at 11.

[6] Blooston at 2.

[7] NCTA at 5. A harm-based trigger also allows providers to better focus their resources. *See, e.g.*, ACA at 5 ("a harm-based notification trigger … spar[es providers] the unnecessary time and expense of generating breach notifications that … likely are at best not actionable"); Blooston at 2 (a harm-based trigger allows providers "to better focus their limited resources on data security and ameliorating the harms caused by data breaches"); CCA at 5 (requiring notification for any breach "would be needlessly costly"). It also aligns with other federal and state breach regimes. *See, e.g.*, USTelecom at 3-4; ACA at 3; CTIA at 22; Hamilton at 6-7; JSI at 3-4; Verizon at 9.

[8] USTelecom at 5 n.12; CCA at 4; CrowdStrike at 2; CTIA at 26; ITI at 3; JSI at 3; Verizon at 8; WISPA at 3; WTA at 7-8.

[9] *See, e.g.*, CTIA at 26; ITI at 3; Verizon at 8; WISPA at 3.

must also adopt a harm-based trigger to avoid notice fatigue and to focus law enforcement and provider resources where they are most needed.[10] Expanding the breach definition without also adopting a harm-based trigger could result in more notifications to consumers of breaches unlikely to cause harm, in turn making it more likely that consumers ignore notifications of breaches that could.[11]

Only one commenter, EPIC, suggests that the Commission expand the breach definition without adopting a harm-based trigger.[12] But EPIC fails entirely to address the risks of over-notification and notice fatigue. The Commission's breach notification rule does not exist in a vacuum; consumers receive breach notices from companies across the entire economy. Forcing consumers to sift through notices of breaches that could harm them along with notices of breaches that will not increases the risks of consumers ignoring the former. Worse, consumers generally would receive notifications of harmless breaches only from their phone carrier, as the Commission's rule would stand apart from other existing breach notification regimes that include a harm-based trigger or equivalent.[13]

In fact, despite opposing a harm-based trigger, EPIC's comments focus on describing the actual harm that can occur from certain breaches. Indeed, EPIC appears most concerned about identity theft, as well as fraud facilitated by identity theft.[14] But CPNI breaches that create a risk of identity theft would require notification under a harm-based trigger. In contrast, a "breach"

---

[10] *See, e.g.*, USTelecom at 5 n.12; ACA at 3-4; Blooston at 2; Hamilton at 5-6; NCTA at 6; NTCA at 4-5; Verizon at 10; WISPA at 3-5; WTA at 8.

[11] USTelecom at 4-5.

[12] Comments of the Electronic Privacy Information Center, WC Docket No. 22-21, at 3, 8 (filed Feb. 22, 2023) ("EPIC").

[13] *See, e.g.*, USTelecom at 3-4; Verizon at 8-9.

[14] EPIC at 3-6.

where a retail associate or customer care representative inadvertently and momentarily accesses the wrong customer's account would not.[15] Accordingly, EPIC's concerns about identity theft and fraud would be fully addressed with a harm-based trigger, without also imposing distracting and unnecessary notifications of harmless breaches. Requiring assessment of harmless breaches also would misallocate the limited resources of law enforcement, the Commission, and service providers.

Finally, EPIC suggests that a standard based on "likelihood" of harm is highly malleable, such that covered entities may use different risk calculations and legal analyses to determine whether the threshold is met.[16] EPIC also suggests that a harm-based trigger could slow reporting.[17] However, as USTelecom and others have explained, harm-based triggers are well established under state law.[18] Companies and their vendors have significant experience assessing the likelihood of harm in a breach's aftermath. Indeed, following a breach, companies generally already are engaged in such analysis as they determine their obligations under the myriad breach reporting requirements that apply. For these reasons, EPIC's concerns are entirely unfounded.

## II. COMMENTERS SHOW THAT TAILORED NOTIFICATIONS BEST SERVE AFFECTED CUSTOMERS AND LAW ENFORCEMENT

The record supports flexibility regarding the timing, content, and method of breach notifications to best meet consumers' and law enforcement's needs.

---

[15] Such situation could constitute a "breach" under the NPRM's proposed definition that a "breach" includes "any instance in which a person, without authorization or exceeding authorization, has gained access to, used, or disclosed CPNI." NPRM ¶ 14.

[16] EPIC at 10.

[17] EPIC at 8.

[18] USTelecom at 3-4.

*Timing of Notification.* The record supports affording carriers flexibility on timing of CPNI breach notifications. As an initial matter, no commenter opposes elimination of the seven-day waiting period, and many affirmatively support the Commission's proposal to eliminate it.[19] Without the mandatory waiting period, carriers in some circumstances will be able to provide customers notice of a breach more quickly than they otherwise could.[20]

The record also makes clear the importance of general flexibility with regard to when carriers notify customers and government agencies of a confirmed breach. As ITI explains, "[o]rganizations must be able to conduct thorough investigations of suspected data breaches to ascertain the nature and scope of such breach before notifying customers or government agencies."[21] That's because "[s]ecurity events are often complex and ongoing, so assessing such incidents – both their nature and impacts on data – often takes … time."[22] Indeed, allowing carriers to fully investigate an incident before providing notice of the breach reduces the risk of inaccurate or incomplete information.[23] It also avoids circumstances in which premature customer notice could lead to further harm, such as when the breach is a result of a cybersecurity vulnerability.[24] The Commission therefore should adopt its proposals to require providers to

[19] *See, e.g.*, USTelecom at 6; ACA at 12-13; Blooston at 6; CCA at 7; CTIA at 20; Hamilton at 7-8; ITI at 3; Comments of Lincoln Network, WC Docket No. 22-21, at 6 (filed Feb. 22, 2023) ("Lincoln Network"); NCTA at 10; Verizon at 5; WISPA at 9.

[20] *See* CTIA at 20.

[21] ITI at 3.

[22] CTIA at 34.

[23] *See, e.g.*, USTelecom at 7; ITI at 3.

[24] *See* ITI at 3 ("[I]t is important that organizations have time to remediate the vulnerability. Unless the vulnerability is addressed prior to making the incident public, the organization and its customers are susceptible to further harm.").

notify customers of breaches without unreasonable delay and law enforcement agencies as soon as practicable after reasonable determination of a breach.[25]

*Content and Method of Notification.* The record supports continued flexibility regarding the information that carriers should include in a CPNI breach notification.[26] As JSI explains, "carriers know their customers best and should have the flexibility to customize notifications to address customer needs."[27] Indeed, carriers have every incentive to provide readable, customer-friendly notifications to their customers, adjusting notices as needed based on the nature of the any given incident.[28] To that end, there is no suggestion in the record that the Commission's flexible approach to the content of CPNI breach notices has failed to serve consumers, as several commenters note.[29] In fact, the Commission's approach has proven effective. Today, "[i]mpacted customers are already receiving relevant information in a timely matter,"[30] as the Commission's current approach "correctly leave[s] 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."[31]

*Threshold for Notification to the Commission and Law Enforcement.* Several commenters suggest a minimum threshold to trigger obligations to report breaches to the

[25] NPRM ¶¶ 11, 23, 31.

[26] ACA at 14; Blooston at 5-6; CTIA at 32; JSI at 6; NCTA at 11; NTCA at 8; Verizon at 6-7.

[27] JSI at 6.

[28] USTelecom at 8.

[29] *See also* NTCA at 8 (explaining that the current rules have been in effect for almost 15 years and there is no evidence that notices have been deficient).

[30] CTIA at 33.

[31] NTCA at 8. In contrast, a prescriptive, one-size-fits-all approach instead could lead carriers to "do too much or too little in individual circumstances." Verizon at 6.

Commission and law enforcement.[32] As Verizon explains, a "threshold trigger would prevent excessive reporting and enable law enforcement to focus its limited resources on larger breaches causing more harm."[33] CTIA also notes that "adopting a threshold for reporting to the Commission and law enforcement would increase harmonization with state breach notification statutes."[34] USTelecom agrees with such commenters that a threshold trigger is worthy of Commission consideration.

*Notification to Business Customers.* The record also supports allowing carriers to bind themselves by contract to different notification regimes for business customers.[35] The best means for reaching a business customer can differ significantly from the best means to reach a residential customer.[36] An enterprise exemption therefore benefits both customers and service providers.[37]

## III. THE RECORD CONFIRMS THAT THE COMMISSION DOES NOT HAVE THE AUTHORITY TO ESTABLISH A NOTIFICATION RULE BEYOND CPNI

Numerous commenters explain that the Commission cannot and should not establish a rule that imposes obligations for information beyond CPNI.[38] They explain that the Commission's authority is limited to CPNI in the first instance, and that Congressional

[32] Blooston at 4; CTIA at 24-25; NCTA at 7; NTCA at 5; Verizon at 11-12; WISPA at 8-9; WTA at 7.

[33] Verizon at 11-12; *see also* WTA at 7 (a reporting threshold helps to "prevent government resources from being bogged down by the investigation of so many small breach incidents").

[34] CTIA at 24-25.

[35] USTelecom at 9; *see also* Verizon at 7 (explaining format requirements may be impracticable in some contexts).

[36] *See* CCA at 8; *see also* USTelecom at 9.

[37] Comments of Voice on the Net Coalition, WC Docket No. 22-21, at 4 (filed Feb. 22, 2023). Separately, USTelecom agrees with CTIA that the Commission's CPNI authentication requirements are worthy of an update. CTIA at 38.

[38] USTelecom at 10-11; CCA at 2; CTIA at 7-15; ITI at 4; Lincoln Network at 7-19; NCTA at 12-14; WISPA at 6.

disapproval of the Commission's 2016 privacy order bars the Commission from reviving the agency's prior flawed claim of authority.[39] Only one commenter, EPIC, claims that the Commission can impose a broader breach notification rule.[40] EPIC is mistaken.

In urging the Commission to "[a]rticulate its [b]road [d]ata [s]ecurity [a]uthority," EPIC relies solely on references to previous, non-precedential statements by the Commission.[41] EPIC fails entirely to submit any analysis of Section 222 or other provisions to support its view that the Commission has broader data security authority,[42] whereas other commenters provide detailed analyses explaining the agency does not.[43] Further, EPIC ignores that the interpretation of broader FCC authority it references has been subject to longstanding pending challenges.[44]

---

[39] Separately, one comment urges the FCC to address arbitration clauses in this proceeding. Comments of American Association for Justice at al., WC Docket No. 22-21, at 2 (filed Feb. 21, 2023). Because this is outside the scope of the proceeding, the Commission should not and cannot entertain the issue here. This also raises significant questions regarding the scope of the Commission's authority under the Federal Arbitration Act, which also place the issue far outside the scope of the NPRM. Federal Arbitration Act, 9 U.S.C. § 1; *Epic Sys. Corp. v. Lewis*, 138 S. Ct. 1612, 1629 (2018).

[40] EPIC at 7, 12.

[41] *Id.* at 7. EPIC cites the Commission's TerraCom and YourTel Notice of Apparent Liability ("NAL") for support. NALs, however, are not final orders and therefore do not serve as legal precedent. *See* 47 U.S.C. § 504(c); *CBS Corp. v. FCC*, 663 F.3d 122, 130, 150 n.29 (3d Cir. 2011) (referring to an NAL as "non-final until the implicated licensee either declines to dispute the findings in the notice or the licensee's responsive opposition is fully adjudicated" and citing FCC brief describing the contents of the NAL as "tentative conclusions"); *Nat'l Commc'ns. Ass'n v. AT&T*, 1998 U.S. Dist. LEXIS 3198, at *144 (S.D.N.Y. 1998) (ruling that party could not introduce the existence of an NAL as evidence of a violation, citing Section 504 and stating that "[t]he NAL initiates an administrative inquiry and is specifically not a final adjudication on the merits").

[42] In a similar vein, the Commission should dismiss EPIC's suggestion to apply the breach notification requirement to breaches of applicant data, which is neither relevant nor appropriate with regard to CPNI. *See* EPIC at 10. CPNI, by statute, includes certain information about a *customer's* use of telecommunications service that is "made available to the carrier by the customer solely by virtue of the carrier-customer relationship," as well as information contained in bills. 47 USC § 222(h)(1). A carrier has no data regarding an applicant that relates to their use of telecommunications service, and there is no carrier-customer relationship with regard to an applicant. There also are no service bills for a non-customer applicant.

[43] *See, e.g.*, USTelecom at 9-10; CTIA at 10-16; NCTA at 12-14; *see also* CCA at 2-3 (FCC should track Congress's direction and priorities as reflected in Section 222 by focusing on CPNI).

[44] *See* USTelecom at 10 n.25.

EPIC also incorrectly suggests that the Congressional Review Act ("CRA") does not bar the FCC from adopting the proposed rules.[45] EPIC reasons that Congress was concerned about privacy authority that duplicated that of the Federal Trade Commission ("FTC") with respect to broadband internet service providers.[46] That reasoning, however, fails to account for the fact that the FCC's 2016 rules also applied to voice services and, at the time, broadband internet access was classified as a Title II telecommunications service and thus was *not* subject to FTC authority.[47] While it certainly is true that Congress was concerned about *dueling* legal regimes, including inconsistent and overlapping requirements that would apply to non-CPNI categories of information in the wake of the Commission's 2016 order, EPIC mistakes the significance of that animating concern for purposes of this rulemaking. Namely, extending breach notification rules beyond CPNI would exacerbate the risk of overlapping jurisdiction and inconsistency with other laws. Accordingly, such action necessarily would implicate the Commission's authority following the CRA and, in turn, requires caution in this proceeding, including, at a minimum, avoiding the same or similar misstep of making an expansive reading of Section 222.[48]

[45] EPIC at 12.

[46] *Id.*

[47] *See* 15 U.S.C. § 45(a)(2). If EPIC were correct that Congress's concern was overlapping regimes, that would serve as another reason to limit the FCC's rules to CPNI, as other information cited by EPIC (*e.g.*, Social Security Numbers) generally is covered by other breach notification regimes.

[48] *See, e.g.*, USTelecom at 10-11; CTIA at 16-17; ITI at 5.

## IV. CONCLUSION

The record provides overwhelming support for the Commission to adopt a harm-based trigger to avoid risks of over-notification and notice fatigue. A harm-based trigger is particularly important should the Commission expand its "breach" definition. The record also supports affording carriers flexibility with regard to when and how they provide notice of a breach. Finally, the record makes clear that the Commission cannot – and should not – impose a breach notification requirement that reaches information beyond CPNI.

Respectfully submitted,

By: */s Joshua M. Bercu/*
Joshua M. Bercu
Vice President, Policy & Advocacy

B. Lynn Follansbee
Vice President, Strategic Initiatives and Partnerships

Adelia Kim
Legal Intern

USTelecom – The Broadband Association
601 New Jersey Avenue, N.W.
Suite 600
Washington, D.C. 20001
(202) 551-0761

March 24, 2023