USTELECOM | THE BROADBAND ASSOCIATION

December 6, 2023

Ms. Marlene Dortch
Secretary
Federal Communications Commission
45 L Street, NE
Washington, DC 20554

Re: *Data Breach Reporting Requirements*, WC Docket No. 22-21

Dear Ms. Dortch:

On December 4, Diana Eisner and the undersigned of USTelecom – The Broadband Association ("USTelecom") met with Elizabeth Cuttner, Legal Advisor to Chairwoman Jessica Rosenworcel; and Greg Watson, Policy Advisor to Commissioner Brendan Carr. On December 5, we met with Hayley Steffen, Acting Legal Advisor to Commissioner Anna Gomez; and Marco Peraza, Wireline Advisor to Commissioner Nathan Simington. On December 6, we met with Justin Faulb, Chief of Staff and Legal Advisor to Commissioner Geoffrey Starks; and Adam Copeland, Zachary Ross, Kimia Nikserescht, Mason Shefa, and John Visclosky of the Wireline Competition Bureau. During the meetings, we discussed several aspects of the draft Report and Order ("*Draft Order*") in the above-referenced proceeding.[1]

The FCC lacks authority to apply data breach rules to information beyond CPNI. We explained that USTelecom members take data security seriously and long have been leaders in innovating and evolving to protect consumers in our digital world. But, consistent with USTelecom's comments and reply comments in the proceeding, the Federal Communications Commission ("FCC" or "Commission") lacks the authority to extend breach notification rules to information beyond customer proprietary network information ("CPNI").[2] We also explained that it is unnecessary to apply Commission data breach rules beyond CPNI, and doing so can confuse consumers. For the information that is not unique to telecommunications services, namely personally identifiable information ("PII") beyond CPNI, carriers are subject to the same state notification requirements that apply to other entities. PII breach notice requirements unique to telecommunications carriers – and only telecommunications carriers – could mislead consumers about the risks associated with breaches of PII held by entities that are not regulated by the FCC relative to those that are.

Data breach obligations should not apply to information that is not sensitive. The *Draft Order*'s application of breach notice requirements to all PII, including historically non-

[1] *Data Breach Reporting Requirements*, Draft Report and Order, WC Docket No. 22-21, FCC-CIRC2312-06 ("*Draft Order*").

[2] *See* Comments of USTelecom – The Broadband Association, WC Docket No. 22-21, at 9-11 (filed Feb. 22, 2023) ("USTelecom Comments"); Reply Comments of USTelecom – The Broadband Association, WC Docket No. 22-21, at 7-9 (filed Mar. 24, 2023) ("USTelecom Reply Comments").

sensitive PII, is of particular concern, and represents a significant departure from the Communications Act and FCC rules, as well as state law.[3] Under section 222(h)(3), subscribers' names, telephone numbers, and addresses are "subscriber list information."[4] Not only did Congress decline to apply the protections set forth in section 222(c) for CPNI to such information, Congress instead required that carriers in some contexts make such information available "*to any person* upon request for the purpose of publishing directories in any format."[5] It makes no sense to define information as sensitive that, by statute and FCC rule, carriers sometimes must share to "any person" on a nondiscriminatory basis. Nor does it make sense to require notification of breaches of information, such as name and address, that is readily and publicly available in various vast (and legitimate) databases of public information.

State breach notification laws take a very different approach. As detailed in our comments, state notification laws do not generally require notification for breaches of PII alone because such information is not inherently sensitive. Rather, they require that such information is breached with sensitive data, like Social Security Numbers or biometrics.[6] Accordingly, under the draft approach, carriers may need to report breaches – at least to the FCC and law enforcement, if not also to customers – that would not be reportable under state law by other entities, even if the exact same data were breached.

For these reasons and consistent with limits to its authority, the Commission should revise the *Draft Order* to apply only to CPNI. To the extent that the FCC inappropriately declines to do so, it should add language to the *Draft Order* and rule that applies the breach notification obligation only to breaches that involve "sensitive PII." In doing so, the FCC should explain that identifying what PII is sensitive is a fact-based, case-by-case determination. It also should deem information like customer name, address, phone number, email address, and contact information as generally not sensitive.

The Commission should ensure that the harm-based notification trigger serves its intended purpose in avoiding over-notification and notice fatigue. USTelecom strongly supported Commission adoption of a harm-based notification trigger.[7] As the *Draft Order* notes, a harm-based notification trigger not only protects consumers from over-notification, but it also allows carriers, particularly small and rural ones, to focus resources on data security and mitigating any harms caused by breaches rather than generating notifications where harm was unlikely. The *Draft Order* further explains that such an approach is consistent with state law.[8]

---

[3] *See, e.g., Draft Order* ¶ 52 n. 219 (suggesting that "first and last name of a customer, their home or other physical address, email or other online contact information, [and] telephone number" are among types of "sensitive personal information").

[4] 47 U.S.C § 222(h)(3).

[5] *Id.* § 222(e) (emphasis added); *see also* 47 CFR § 64.2309.

[6] *See* USTelecom Comments at 3 (citing as examples Mass. Ann. Laws Ch. 93H, § 1; N.Y. Gen. Bus. Law § 899–aa(1); Del. Code Ann. tit. 6, § 12B-101).

[7] USTelecom Comments at 3-6; USTelecom Reply Comments at 1-4.

[8] *Draft Order* ¶ 49.

But as constructed in the *Draft Order*, the harm-based notification trigger does not set forth reasonable parameters for carriers to assess risk. Notably, the criteria that carriers are required to consider in overcoming the rebuttable presumption of harm include highly-context-specific factors that carriers almost never will know, such as the possibility for mental pain and emotional distress.[9] This is compounded by the expansive breadth of data that inappropriately would be covered by the *Draft Order*'s breach notification rule, as discussed above. The *Draft Order* therefore still poses significant risk of over-notification to customers, causing notice fatigue, Rather than create a rebuttable presumption of harm, the *Draft Order* should more closely track analogous state laws that do not establish a presumption of harm, and simply exempt from notification obligations any breaches where harm is not reasonably likely. Many of these laws also construe harm significantly more narrowly. In addition, to better align with state laws, the harm-based notification trigger should automatically exclude incidents involving encrypted data when there is no reason to believe that the underlying data can be accessed.[10]

The harm-based notification trigger should apply to notification to the FCC and law enforcement. Separately, the same rationales for a harm-based notification trigger apply equally to notification to the FCC and law enforcement.[11] First, just as it would be for consumers, it is an inefficient use of FCC and law enforcement resources to review notifications of breaches that are unlikely to result in harm to consumers. This is particularly acute given the draft's expanded definition of "breach" to include inadvertent exposure of information, as well as the draft's inappropriate expansion to all PII regardless of sensitivity or encryption. To require carriers to notify the Commission of a breach of encrypted data serves no purpose. Also, in the annual summary to the FCC and law enforcement about small breaches,[12] carriers arguably would need to report each and every time that a customer agent left out a document that had one customer's name, resulting in recordkeeping and notification to law enforcement of thousands and thousands of "breaches" that do not pose any possibility of harm. Second, such broad reporting – as well as the underlying recordkeeping it de facto requires – is an inefficient use of carrier resources, and could divert resources from more impactful efforts to enhance data security and mitigate any harms caused by breaches. Finally, state breach notification laws generally do not require notification of harmless security incidents to law enforcement.

* * *

[9] *Id.* ¶ 51.

[10] *See, e.g.,* Cal Civ. Code § 1798.82(a) (excluding from notification requirements breach of encrypted personal information unless the key or security credential also is acquired); Mass. Gen. Laws 93H sec. 1(a) (excluding from "breach of security" definition breaches of encrypted data unless the confidential encryption process or key also is acquired).

[11] *See Draft Order* ¶ 49 (harm-based notification trigger (i) ensures that customers are aware of potentially harmful instance of breach while preventing unnecessary financial and emotional difficulty in no-harm situations; (ii) allows carriers, particularly small and rural providers, to focus resources on data security and mitigating any harms caused by breaches; and (3) is consistent with the majority of state laws).

[12] *See id.* ¶ 37.

Please contact the undersigned with any questions.

Sincerely,

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