The FCC's New Data Breach Notification Rules

John T. Nakahata, Jennifer P. Bagg, Adrienne E. Fowler, and Daeyeong Kim

Earlier this week, the Federal Communications Commission's Report and Order adopting new data breach notification rules for telecommunications, interconnected VoIP (collectively, "carriers"), and telecommunications relay service ("TRS") providers ("covered providers") was published in the Federal Register. Although the effective date of the Report and Order has been set as March 13, 2024, substantive changes to the FCC's data breach notification regulations are on hold due to ongoing Office of Management and Budget review. Nonetheless, affected providers should be preparing for these requirements in advance if they cannot already meet them: as we outline below, the new rules represent a significant expansion of providers' data-breach-related obligations.

Expansion of the types of information that is subject to a data breach reporting requirement. Currently, FCC data breach reporting rules only require covered providers to report data breaches impacting customer proprietary network information ("CPNI"),[1] which is a limited subset of service-related information that providers collect from their customers.[2] The new rules apply to the breach of personally identifiable information ("PII"), which is a much broader category of data than CPNI.[3] Examples of PII include the following: an individual's first name (or first initial) and last name, in combination with any government-issued identification numbers or information issued on a government document used to verify the individual's identity, or other unique identification numbers used for authentication purposes; username or email address in combination with a password or security question and answer; and unique biometric, genetic, or medical data.[4] For TRS providers, covered data also includes the content of any relayed conversation.[5]

Expansion of the types of incidents that qualify as a reportable "breach." Under the current rules, "breach" is limited to when a person *intentionally* gains access to, uses, or discloses covered data.[6] The Commission revised its definition of a "breach" to include inadvertent access, use, or disclosure of covered data.[7] The new rules also create an exception for good-faith acquisitions of covered data by an employee or agent of a carrier or TRS provider, if the information is not used improperly or further disclosed.[8] The Commission emphasized, however, that it expects carriers and TRS providers to take reasonable measures to guard against improper use and/or further disclosure such as requiring the employee or agent to destroy the improperly disclosed data.[9]

---

[1] 47 C.F.R. § 64.2011(e)(2*)*; *id.* § 64.5111(e)(2).

[2] 47 U.S.C. § 222(h)(1) (defining CPNI as "(A) information that relates to the quantity, technical configuration, type, destination, 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 service received by a customer of a carrier; except that such term does not include subscriber list information").

[3] *To be codified at* 47 C.F.R. § 64.2011(e)(2); *id.* § 64.5111(e)(2).

[4] *To be codified at id.* § 64.2011(e)(5)–(6).

[5] *To be codified at id.* § 64.5111(e)(2).

[6] 47 C.F.R. § 64.2011(e); *id.* § 64.5111(e).

[7] *To be codified at id*. § 64.2011(e)(1); *id.* § 64.5111(e)(1).

[8] *To be codified at id.* § 64.2011(e)(1); *id.* § 64.5111(e)(1).

[9] *Data Breach Reporting Requirements*, WC Docket No. 22-21, Report and Order, FCC 23-111, ¶ 26 n.98 (2023) ("*Data Breach Order*").

Changes to when and how providers must notify to federal agencies. Under the new rules, covered providers only need to report a subset of breaches to federal agencies. Reportable breaches include: (i) breaches that affect 500 or more customers; (ii) breaches for which the number of affected customers is unknown; (iii) breaches for which there is a reasonable risk of harm, regardless of the number of affected customers; and (iv) breaches for which the provider initially determines notification is not required, but later discovers information that requires notification.[10]

If a breach involves fewer than 500 customers *and* the provider reasonably determines that no harm to affected customers is reasonably likely to occur, the provider does not need to submit a specific notification to federal agencies; however, the provider must include a description of such breaches as part of an annual summary.[11]

When a notification is required, it must include (i) the provider's address and contact information; (ii) a description of the breach incident; (iii) the method of compromise; (iv) the date range of the incident; (v) the approximate number of customers affected; (vi) an estimate of financial loss to the carrier and customers, if any; and (vii) the types of data breached.[12] TRS providers must also include a description of the breached customer information that specifically discusses whether call content, such as call transcripts, was exposed.[13] Additionally, a carrier must update its initial breach notification report if it learns that the report was materially incomplete or incorrect, or if additional information becomes known to the carrier.[14]

Changes to when and how providers must notify customers. The new data breach notification rules adopt a harm-based trigger for notifications to customers. As such, if (i) a covered provider reasonably determines that no harm to customers is reasonably likely to occur as a result of the breach or (ii) the breach solely involves encrypted data and the provider has *definitive* evidence that the encryption key was not accessed, the provider is not required to notify its customers.[15] When evaluating harm, the provider must consider factors such as the sensitivity of the breached information, the nature and duration of the breach, mitigations, and intentionality when evaluating the likelihood of harm.[16] TRS providers must assume that harm has occurred or is reasonably likely to occur if call content (e.g., call audio, transcripts) has been or has the potential to be disclosed as a result of the breach.[17]

Any customer notification must occur without unreasonable delay after notification to federal agencies, and no longer than thirty days after reasonable determination of a breach, unless law enforcement requires a longer delay.[18]

The customer notification must include "sufficient" information that would make a reasonable customer aware that a breach occurred on a certain date and that the breach may have affected the customer's data.[19] The Commission recommends that the notification contain the following categories of information: (i) estimated date of the breach; (ii) description of the customer data that was accessed (for TRS providers, include also whether data on the contents of conversations such as call transcripts were accessed); (iii) information on how customers (including customers with disabilities) can contact the provider to inquire about the breach; (iv) information about how to contact the FCC, Federal Trade Commission, and any relevant state regulatory

---

[10] *Data Breach Order* ¶¶ 31, 84–85.

[11] *To be codified at* 47 C.F.R. § 64.2011(d); *id.* § 64.5111(d).

[12] *To be codified at id.* § 64.2011(a)(1); *id.* § 64.5111(a)(1).

[13] *To be codified at id.* § 64.5111(a)(1).

[14] *Data Breach Order* ¶ 42.

[15] *To be codified at* 47 C.F.R. § 64.2011(b); *id.* § 64.5111(b).

[16] *Data Breach Order* ¶¶ 57, 99.

[17] *Data Breach Order* ¶ 99.

[18] *To be codified at* 47 C.F.R. §§ 64.2011(a)(2), (b); *id.* §§ 64.5111(a)(2), (b). The new rule removes the mandatory seven-day waiting period of the current rule. 47 C.F.R. § 64.2011(b)(1); *id.* § 64.5111(b)(1).

[19] *To be codified at id.* § 64.2011(b); *id.* § 64.5111(b).

agencies; (v) if the breach creates a risk of identity theft, information about national credit reporting agencies and steps to guard against identify theft; and (vi) other steps customers should take to mitigate their risk.[20]

* * * *

For more information on the FCC's data breach notification requirements or our telecommunications practice, please contact John Nakahata, Jennifer Bagg, Adrienne Fowler, Daeyeong Kim, or the HWG attorney with whom you regularly work.

[20] *Data Breach Order* ¶¶ 63, 112.