FCC Seeks Comments on Updates to CPNI Breach Reporting Rule

Aaron J. Burstein, Alexander I. Schneider

January 24, 2023

The Federal Communications Commission ("FCC" or "Commission") is seeking comments on a Notice of Proposed Rulemaking (NPRM) to refresh its customer proprietary network information ("CPNI") data breach reporting requirements (the "Rule"). Adopted earlier this month by a unanimous 4-0 vote of the Commission, the NPRM solicits comments on rule revisions that would expand the scope of notification obligations and accelerate the timeframe to notify customers after a data breach involving telephone call detail records and other CPNI. The FCC cites "an increasing number of security breaches of customer information" in the telecommunications industry in recent years and the need to "keep pace with today's challenges" and best practices that have emerged under other federal and state notification standards as reasons to update the Rule.

According to the current Rule, a "breach" means that a person "without authorization or exceeding authorization, has intentionally gained access to, used, or disclosed CPNI." As summarized in the NPRM, CPNI includes "phone numbers called by a consumer, the frequency, duration, and timing of such calls, the location of a mobile device when it is in active mode (i.e., able to signal its location to nearby network facilities), and any services purchased by the consumer, such as call waiting." (The NPRM does not propose any changes to the definition of CPNI.)

Initially adopted in 2007 as part of a broader effort to combat pretexting – the practice of pretending to be a customer in order to obtain that customer's telephone records – the current data breach notification rule (47 CFR § 64.2011) requires telecommunications carriers, including interconnected VoIP providers, to provide notice of a data breach involving CPNI to the Secret Service, FBI, and affected customers. The Rule also requires notifying law enforcement within seven business days at http://www.fcc.gov/eb/cpni. Carriers then must wait an additional seven business days to notify customers about a breach (barring any objection from law enforcement officials).

The NPRM solicits comments on a series of potential changes to the Rule, including:

- **Removing the intent standard:** Under the current Rule, a breach is reportable when a person *intentionally*, and without authorization or exceeding authorization, gains access to, uses, or discloses CPNI. The NPRM proposes removing the intent standard, explaining that "inadvertent" disclosures of CPNI can still impact individuals, and that intent may not be immediately apparent "which may lead to legal ambiguity or under-reporting." The FCC seeks comments on the benefits and burdens of this proposal and whether other data breach laws should influence the policy it adopts.

- **Adding a harm-based reporting trigger:** The FCC proposes to include a harm-related reporting trigger, in an effort to avoid notifying customers about breaches that are not likely to

cause harm – what the FCC terms “notice fatigue.” As an example, many data breach laws do not require notification about a data breach involving encrypted information based in part on a harm calculation. The FCC also solicits comments on how to determine and quantify “harm” in the context of CPNI.

- **Expanding the notice requirement:** The NPRM asks whether the FCC has authority to include in its Rule – and should include – information that is not considered CPNI, such as Social Security numbers or other financial records,.
- **Notice to the FCC:** The FCC proposes that carriers should notify the FCC, in addition to the FBI and Secret Service, about CPNI breaches. It seeks comment on the costs and benefits of requiring such notification.
- **Notice Timeline:** The FCC proposes removing the seven-business day waiting period to notify customers about a CPNI data breach, instead requiring notification “without unreasonable delay” after discovery of a breach, unless a law enforcement agency requests that the carrier delay notification. The FCC tentatively concludes this approach is consistent with other laws and better serves the public interest than the current requirement.
- **Minimum Requirements for Notice Content:** The current rule does not address the content of notifications, and the NPRM solicits comment on whether to adopt a floor for information that must be included in data breach notices to consumers. The FCC notes that many state data breach notification laws impose minimum content requirements, requiring notices to describe what information was subject to the breach, the date(s) of the breach, how the breach occurred, and what steps were taken to remedy the situation.

Finally, the NPRM raises the question of the FCC’s legal authority to adopt its proposed changes to its Rule, particularly in light of the fact that Congress nullified the 2016 revisions to its Rule (*2016 Privacy Order*) under the Congressional Review Act.

Comments on the NPRM are due on February 22, and reply comments are due on March 24.