wiley

ALERT

FCC Releases Long-Anticipated Data Breach Reporting NPRM, Proposing Major Changes to CPNI Rules

January 9, 2023

On January 6, 2023, the Federal Communications Commission (FCC or Commission) released its *Data Breach Reporting Requirements NPRM* (*NPRM*) after adopting the item by a 4-0 vote on December 28, 2022. This long-awaited NPRM proposes major changes to the FCC's regulation of customer data and takes place against a backdrop of substantial federal and state activity on incident and data breach reporting, including at the Federal Trade Commission, the Department of Homeland Security and the Securities and Exchange Commission.

FCC Chairwoman Jessica Rosenworcel first placed this item on circulation on January 12, 2022 – nearly one year ago. The *NPRM* proposes substantial changes to the Commission's customer proprietary network information (CPNI) breach reporting rules – 47 C. F.R. § 64.2011 – including proposals to: expand the definition of the term "breach" to include accidental access, use, or disclosure; require breach notification to the FCC, FBI, and Secret Service "as soon as practicable" after the discovery of a breach; eliminate the mandatory seven-business-day waiting period prior to customer notification and adopt minimum requirements that must be contained in CPNI breach notices made to customers; and extend the same proposed changes to the CPNI breach reporting rule to the Telecommunications Relay Services (TRS) breach reporting rule – 47 C.F.R. § 64.5111. Notably, the *NPRM* asks whether the Communications Act gives the Commission the authority to establish breach reporting obligations for customer Social Security Numbers (SSNs) and financial records possessed by telecommunications carriers.

Authors

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Kevin G. Rupy
Partner
202.719.4510
krupy@wiley.law

Stephen J. Conley
Associate
202.719.4572
sconley@wiley.law

Practice Areas

Privacy, Cyber & Data Governance
Telecom, Media & Technology

There are many complex issues raised in the NPRM, which we analyze below. Comments will be due 30 days after publication in the Federal Register, and reply comments are due 60 days after publication.

The FCC's Existing CPNI Rules and Enforcement Role

The FCC has long regulated CPNI at the express direction from Congress in Section 222 of the Communications Act, enacted in 1996. While the FCC left many definitional and interpretive issues to regulated entities, the agency has been publicly increasing pressure on telecommunications carriers to do more to protect consumer data. The agency has in the past sought to expand its role in protecting consumer data, through rules overturned by Congress and in a series of enforcement proceedings leading to consent decrees with varying terms. In this NPRM, the agency appears intent on confirming its increasingly expansive approach and increasing the expectations for regulated entities.

Section 222(h)(1) of the Communications Act defines 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.

In the *2007 CPNI Order*, the FCC explained that this type of information 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. As part of the *2007 CPNI Order*, the Commission revised its rules to, among other things, require telecommunications carriers to notify FBI and Secret Service and customers of CPNI breaches. *2007 CPNI Order* ¶¶ 26-32. The rules specifically require reporting to the FBI and Secret Service of a CPNI breach within seven business days after a reasonable determination of the breach. Telecommunications carriers may notify customers after seven business days following notification to FBI and Secret Service.

Some commentators and previous agency leadership wanted the agency to do more to protect broader types of information and to regulate entities beyond traditional telecommunications companies.

In the *2016 Broadband Privacy Order*, the Commission greatly expanded its breach notification rule. This expansion would have regulated a wide range of information, including personally identifiable information and the contents of communications, in addition to the categories of CPNI identified in the *2007 CPNI Order*. *2016 Broadband Privacy Order* ¶ 46. And it would have imposed these obligations on ISPs in addition to telecommunications carriers. *Id.* ¶ 19. However, Congress nullified the *2016 Broadband Privacy Order* in 2017 through use of the Congressional Review Act (CRA).

The agency has used its enforcement authorities to review CPNI practices after incidents and has used those enforcement actions to attempt to expand its reach. In a series of actions, most resulting in negotiated consent decrees, the agency has imposed substantial forfeitures for allege failures to safeguard CPNI and, in

some actions has asserted authority over personal information that does not meet the definition of CPNI.

***NPRM* Summary and Analysis**

The NPRM states that changes are needed to "better protect telecommunications customers and ensure that our rules keep pace with today's challenges" so the agency is "propos[ing] a number of updates to our rule addressing telecommunications carriers' breach notification duties." *NPRM* ¶ 10. The NPRM proposes several changes and expansions to key concepts and duties.

The Proposal Would Expand the Definition of "Breach." The *NPRM* proposes to expand the FCC's definition of "breach" in its CPNI rules "to include inadvertent access, use, or disclosures of customer information." *NPRM* ¶ 12. Specifically, the *NPRM* would revise the definition of a "breach" to include "any instance in which a person, without authorization or exceeding authorization, has gained access to, used, or disclosed CPNI." *Id.* ¶ 14. The current rule defines a CPNI "breach" as "when a person, without authorization or exceeding authorization, has intentionally gained access to, used, or disclosed CPNI." 47 C.F.R. § 64.2011(e).

The Agency Asks About Using a Harm-Based Notification Trigger. The *NPRM* also seeks comment on "whether to forego requiring notification to customers or law enforcement of a breach . . . where a telecommunications carrier can reasonably determine that no harm to customers is reasonably likely to occur as a result of the breach." The *NPRM* further asks whether harm should be quantified to include "reputational damage, personal embarrassment, and loss of control over the exposure of intimate personal details. . . ." *Id.* ¶ 15. The *NPRM* proposes that if the Commission adopts a harm-based trigger and a carrier is unable to make a harm determination or is uncertain about whether harm would be likely to occur, then the breach notification obligation would remain. *Id.* ¶ 21. The current CPNI breach notification rule requires no showing of harm.

The Commission Inquires About its Authority to Require Breach Reporting for SSNs and Other Financial Information. The *NPRM* also seeks comment on whether the FCC has the authority to establish breach-reporting obligations under Section 222 for SSNs and financial records. Additionally, the *NPRM* asks how to define the "proprietary information" that carriers would be required to report if the Commission were to require reporting of SSNs and other financial information. *Id.* ¶ 22.

The Agency Would Expand Breach Notification to the FCC, in Addition to Law Enforcement. The *NPRM* next proposes to require carriers to "notify the Commission of breaches, in addition to the Secret Service and FBI, as soon as practicable. . . ." *Id.* ¶ 23. Additionally, the *NPRM* tentatively concludes that notification of breaches will provide FCC staff "important information about data security vulnerabilities" and that such notification will "shed light on carriers' ongoing compliance with [FCC] rules." *Id.* ¶ 24. The NPRM also proposes to "create and maintain a centralized portal for reporting breaches to the Commission and other federal law enforcement agencies," as the current CPNI breach reporting rules only require reporting to the FBI and Secret Service. *Id.* ¶ 25.

The Agency Seems Inclined to Maintain Current Notification Content Requirements. The FCC's CPNI central reporting facility currently requires carriers to report information relevant to the breach, including carrier contact information; a description of the breach incident; the method of compromise; the date range of the incident, approximate number of customers affected; an estimate of financial loss to the carriers and customers, if any; types of data breached; and the addresses of affected customers. The *NPRM* states that the Commission believes this information is "largely sufficient," but asks for feedback. *Id.* ¶ 27.

The New Rule Would Require Contemporaneous Notice to the FCC and Asks About Changes to Required Timing and Triggers. Presently, the rules require notice through the FCC to law enforcement. The *NPRM* proposes "to require carriers to notify the Commission of a reportable breach contemporaneously with notification to other law enforcement agencies as soon as practicable after discovery of a breach." *Id.* ¶ 28. The NPRM asks about possible changes to the required timing, from within seven days to "as soon as practicable" or using 24 or 72 hours as the standard, in addition to "when a carrier should be treated as having 'reasonably determined' that a breach has occurred." *Id*.

The Agency Contemplates a Numerical Reporting Threshold. The *NPRM* also seeks comment on whether to set a threshold for the number of affected customers to trigger breach reporting to the Commission, FBI, and Secret Service. *Id.* ¶ 29. The current CPNI breach reporting rules do not specify a customer threshold, so this could be a really practical way to limit obligations to larger and more substantial breaches.

The Agency Would Change the Timing for Customer Notifications. The *NPRM* proposes to require carriers to notify customers of CPNI breaches "without reasonable delay after discovery of a breach and notification to law enforcement, unless law enforcement requests a delay" in customer reporting. *Id.* ¶ 31. The *NPRM* tentatively concludes that the mandatory seven-business-day customer notification period "is out-of-step with current approaches regarding the urgency of notifying victims about breaches of their personal information" and also tentatively concludes that its proposal "better serves the public interest" than the current rule. *Id.* ¶ 32.

The Agency May Regulate the Form and Contents of Customer Breach Notifications. The *NPRM* seeks comment on whether the Commission should require carriers to include specific information in customer CPNI breach notifications. While the current rules specify when and to whom customer breach notifications must be made, they do not dictate the contents. The *NPRM* seeks comment on requiring the following information at a minimum: (1) the date of the breach; (2) a description of the customer information that was used, disclosed, or accessed; (3) information on how customers, including customers with disabilities, can contact the carrier to inquire about the breach; (4) information about how to contact the Commission, FTC, and any state regulatory agencies relevant to the customer and the service; (5) if the breach creates a risk of identity theft, information about national credit reporting agencies and the steps customers can take to guard against identity theft, including any credit monitoring, credit reporting, or credit freezes the carrier is offering to affected customers; and (6) what other steps customers should take to mitigate their risk based on the specific categories of information exposed in the breach. *Id.* ¶ 40.

The *NPRM* also seeks comment on whether the FCC should adopt a particular required breach notification method (*i.e.*, mail, email, telephone etc.). *Id.* ¶ 41.

The Agency May Extend the NPRM to Telecommunications Relay Service (TRS) CPNI. The agency presently has slightly different rules regarding CPNI in the context of TRS services. The *NPRM* seeks comment on the Commission's authority to extend its CPNI breach reporting rule proposals to its TRS breach reporting rules – 47 C.F.R. § 64.5111. Specifically, the *NPRM* proposes to (1) to expand the Commission's definition of "breach" to include inadvertent disclosures of customer information; (2) to require TRS providers to notify the Commission, in addition to the Secret Service and FBI, as soon as practicable after discovery of a breach; and (3) to eliminate the mandatory waiting period to notify customers, instead requiring TRS providers to notify customers of CPNI breaches without unreasonable delay after discovery of a breach unless law enforcement requests a delay. *Id.* ¶ 42.

The Agency Asks About its Legal Authority to Take Several of the Actions in the NPRM. The source and scope of the Commission's authority to regulate beyond the relatively narrow category of CPNI has been contested and unsettled, invoked as it has been in sporadic enforcement actions but not reflected in agency rules. The *NPRM* tentatively concludes that Section 222 provides the Commission with the authority to adopt its proposed breach notification rules, and breach notification rules for which the *NPRM* seeks comment on. *Id.* ¶ 46. In support of this conclusion, the *NPRM* cites Section 222(a), which imposes a duty on carriers to "protect the confidentiality of proprietary information of, and relating to" customers, other carriers, and manufacturers. 47 U.S.C. § 222(a).

The NPRM Asks About the Implications of the 2016 Broadband Privacy Order and CRA Action. Finally, the *NPRM* seeks comment "on the effect and scope" of the 2017 CRA of the *2016 Broadband Privacy Order* "for the purpose of adopting rules that apply to telecommunications carriers. *Id.* ¶ 52. The Commission's *2016 Broadband Privacy Order* adopted expansive privacy rules covering both broadband Internet access providers and telecommunications carriers under Section 222 of the Communications Act. Specifically, the *2016 Broadband Privacy Order* would have defined CPNI broadly to include customer information such as IP and MAC addresses and would have required telecommunications carriers to report breaches of personally identifiable information, including SSNs and customer financial information. However, the use of the CRA on the *2016 Broadband Privacy Order* prevents the FCC from "reissu[ing] . . . in substantially the same form," or on issuing "a new rule that is substantially the same as," the *2016 Broadband Privacy Order*. 5 U.S.C. § 801(b)(2). Accordingly, the FCC's conclusion in the *NPRM* that it has the legal authority to adopt rules requiring telecommunications carriers to report breaches involving SSNs and other customer financial information is likely to face legal questions from industry stakeholders.

This Rulemaking Is One of Many Cybersecurity and Incident Reporting Efforts

This *NPRM* asks a variety of important questions and makes substantial proposals that will affect incident reporting and the substantive regulation of various kinds of data by the FCC. This Rulemaking is taking place at the same time that the Federal Trade Commission is considering whether to adopt major new rules for private sector data use, security, and reporting. The Department of Homeland Security has also started its

proceeding to implement major new cyber incident reporting requirements at the direction of Congress in the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA). And the Securities and Exchange Commission has proposed cyber incident reporting rules.

As the Chairwoman leads the Federal Interagency Cybersecurity Forum, and the Cyber Incident Reporting Council looks at harmonization and deconfliction of reporting obligations, this FCC data breach proceeding takes on additional significance. It will be important for industry to share practical experiences with the FCC to help the agency calibrate obligations and avoid unnecessary duplication or overlap that can burden companies experiencing a cyber incident or data breach.

***

For more information about the *NPRM* or filing comments, please contact any of the authors listed on this alert.