Updates
January 12, 2023
FCC Proposes To Strengthen Data Breach Notification Rules for Telecom Operators

In response to the increased frequency and severity of data breaches in the telecommunications industry, the Federal Communications Commission recently published a Notice of Proposed Rulemaking that seeks to strengthen and broaden its breach notification rules arising from the unauthorized disclosure of customer proprietary network information (CPNI). This rulemaking is the first effort by the FCC to update its notification rules since these were adopted nearly two decades ago. These rules apply to providers of telecom services (i.e., telecom carriers). Generally, CPNI is defined as certain individually identifiable customer information received or obtained by a telecom carrier during the carrier-customer relationship. The FCC intends to better align its data breach notification rules with federal and state data breach notification laws that cover other industries. In particular, the FCC proposes the following:

- Expanding the definition of "breach" to include inadvertent access, use, or disclosure of customer information.
- Adding a requirement that, in addition to federal law enforcement, the FCC be notified of breaches in a timely manner.
- Eliminating the mandatory seven-day waiting period before notifying customers of a breach.

Revising the Definition of "Breach"

The FCC proposes expanding the rule's definition of "breach" to include inadvertent access, use, or disclosures of customer information. The current rule excludes accidental breaches by defining a "breach" as an "intentional" access, use, or disclosure.

In support of this proposed change, the FCC noted that growing experience with data breaches has demonstrated that inadvertent exposure of customer information can result in the loss and misuse of sensitive information as well. The FCC also noted that it may not always be immediately apparent whether a breach was intentional or not, which could lead to legal ambiguity or underreporting under the current rule. Finally, the FCC underscored the importance of notifying law enforcement of any accidental access, use, or disclosure. That way, both law enforcement and the FCC can investigate and advise carriers on how to avoid future breaches, as well as be ready to respond if the affected information falls prey to malicious actors.

The FCC seeks comment on whether it should expand the definition of "breach" to include situations where a carrier or third party discovers conduct that could have reasonably led to exposure of CPNI, even if it has not yet determined whether such exposure occurred. Additionally, the FCC seeks comment on whether to forego requiring notification of a breach in those instances where a carrier can reasonably determine that no harm to customers is likely to occur as a result of the breach (i.e., whether to adopt a "harm-based notification trigger").

Adding a Requirement To Notify the FCC

The FCC proposes requiring carriers to notify the FCC itself of breaches, in addition to notifying the U.S. Secret Service and Federal Bureau of Investigation (FBI), as required by the current rule.

The FCC explains that the updated rule would be consistent with other federal data breach laws, which require notification to relevant subject matter agencies (e.g., data breach notification requirements under the Health

Insurance Portability and Accountability Act generally require notice to the U.S. Department of Health and Human Services). The FCC contends that receiving notifications of breaches would provide its staff with important information about data security vulnerabilities so staff, in turn, could help address and remediate the vulnerabilities. Additionally, the FCC notes that breach notifications would likely shed light on carriers' ongoing rules compliance.

The FCC also seeks comment on other aspects of the notice requirements, such as the following:

- How the rules can minimize potentially duplicative data breach reporting burdens for carriers, particularly given the recent passage of the Cyber Incident Reporting for Critical Infrastructure Act of 2022, which requires covered entities to notify the U.S. Department of Homeland Security of certain cybersecurity incidents.
- Whether notifications to the FCC should follow the same requirements as currently required for notifications to federal law enforcement agencies. (The FCC tentatively concluded they should be the same.)
- What the appropriate timeframe for notifying the FCC and other federal law enforcement of a breach should be. (The FCC tentatively concluded requiring carriers to notify it of a reportable breach "contemporaneously" with notification to other law enforcement agencies "as soon as practicable" after discovery of a breach.)
- Whether it is appropriate to set a minimum threshold requirement for the number of affected customers before a carrier must report a breach to the FCC.

Eliminating Mandatory Waiting Period for Notifying Customers

The FCC proposes requiring carriers to notify customers of CPNI breaches "without unreasonable delay" after the carrier discovers the breach and first notifies law enforcement, although the proposed rules also would allow the FBI or Secret Service to direct a carrier to delay customer notification for an initial period of up to 30 days if such notification would interfere with a criminal investigation or national security. The current rule prohibits carriers from notifying customers or disclosing the breach to the public until at least seven full business days after notification to the Secret Service and FBI.

While noting that the existing rule is grounded in concerns that customer notification may make a breach public, thereby impeding law enforcement's ability to investigate, the FCC acknowledges that this concern is out of step with current approaches regarding the urgency of notifying victims about breaches of their personal information. The FCC proposes that replacing the seven-day waiting period with a "without unreasonably delay" standard would better serve the public interest because it would permit customers to receive important information more quickly.

Regarding the specifics of its proposed customer notification requirement, the FCC seeks comment on issues including:

- Whether the "without unreasonably delay" standard provides carriers with enough time to determine the scope and impact of a breach, as well as with sufficient guidance as to the required timeframe to notify customers. (Telecoms may also reasonably question whether this standard is sufficiently clear or carries the risk of unfair or arbitrary enforcement.)
- Whether the same notification deadline should be applied to all carriers, regardless of their size.
- Whether carriers should be allowed to notify customers and law enforcement notification at the same time in certain situations.

Other Proposals

In addition to these three proposals discussed above, the FCC proposes to make equivalent amendments to similar rules that apply to Telecommunications Relay Services (TRS), which allows individuals who are deaf, hard of hearing, deafblind, or have speech disabilities to communicate by telephone in a manner that is functionally equivalent to telephone services used by persons without such disabilities.

The FCC also seeks comment on whether it should require customer notifications to include specific information about the breach (e.g., a description of the customer information that was used, disclosed, or accessed), as well as whether it should require that notifications to customers take a certain form (e.g., physical mail, email, or telephone).

Takeaways

This FCC rulemaking proceeding is the cumulation of a year-long effort by the FCC to modernize its CPNI data breach notification requirements to more closely align with similar laws at the federal and state levels, as well as to better reflect industry best practices. Adopted by a unanimous vote by a politically divided FCC, it reflects the widely held concern about the damaging effects of data breaches for consumers and the industry.

Comments are due 30 days after the NPRM is published in the *Federal Register*, with reply comments due 60 days after publication. Publication is expected to occur within the next few weeks, which will likely result in comments being due sometime in March and reply comments in April.

Authors

Explore more in

Privacy & Security Technology Transactions & Privacy Law Communications

Related insights

Update

California Court of Appeal Casts Doubt on Legality of Municipality's Voter ID Law

Update

New US Commerce Prohibitions on Chinese and Russian Connected Vehicle Technology