

Media Contact:

Paloma Perez

Paloma.Perez@fcc.gov

For Immediate Release

**CHAIRWOMAN ROSENWORCEL CIRCULATES NEW DATA
BREACH REPORTING REQUIREMENTS**

***Proposal is a Response to Recent Security Breaches in the Telecommunications
Industry***

WASHINGTON, January 12, 2022—Today Federal Communications Commission Chairwoman Jessica Rosenworcel shared with her colleagues a Notice of Proposed Rulemaking (NPRM) that would begin the process of strengthening the Commission’s rules for notifying customers and federal law enforcement of breaches of customer proprietary network information (CPNI). The updates would better align the Commission’s rules with recent developments in federal and state data breach laws covering other sectors.

“Current law already requires telecommunications carriers to protect the privacy and security of sensitive customer information. But these rules need updating to fully reflect the evolving nature of data breaches and the real-time threat they pose to affected consumers,” said Chairwoman Rosenworcel. “Customers deserve to be protected against the increase in frequency, sophistication, and scale of these data leaks, and the consequences that can last years after an exposure of personal information. I look forward to having my colleagues join me in taking a fresh look at our data breach reporting rules to better protect consumers, increase security, and reduce the impact of future breaches.”

The proposal outlines several updates to current FCC rules addressing telecommunications carriers’ breach notification requirements. These include:

- Eliminating the current seven business day mandatory waiting period for notifying customers of a breach;
- Expanding customer protections by requiring notification of inadvertent breaches; and
- Requiring carriers to notify the Commission of all reportable breaches in addition to the FBI and U.S. Secret Service.

The increasing frequency and severity of security breaches involving customer information can have lasting detrimental impacts on the economy and on consumers whose information has been improperly exposed. To reduce the risk of this harm, in September, the FCC proposed rules targeting SIM swapping scams and port-out fraud.

The Notice of Proposed Rulemaking circulated today further advances the FCC’s efforts to ensure its rules keep pace with evolving cybersecurity threats and to protect consumers in the face of today’s challenges. The proposal also aims to ensure that the Commission and other federal law enforcement agencies receive the information they need in a timely manner so they can mitigate and prevent harm due to the breach and take action to reduce the likelihood of future incidents. Lastly, the Notice also seeks comment on whether the Commission should require customer breach notices to include specific categories of information to help ensure

they contain actionable information useful to the consumer and proposes to make consistent revisions to the Commission's telecommunications relay services (TRS) data breach reporting rule.

###

Media Relations: (202) 418-0500 / ASL: (844) 432-2275 / Twitter: @FCC / www.fcc.gov

This is an unofficial announcement of Commission action. Release of the full text of a Commission order constitutes official action. See MCI v. FCC, 515 F.2d 385 (D.C. Cir. 1974).