DATASHEET

Radar® Privacy

FCC Breach Notification Rules in Radar® Privacy

Stay compliant with FCC requirements for telecommunications companies.

The FCC's Breach Notification Rules have provided customers of telecommunications carriers and telecommunications relay services (TRS) providers protection against the misuse or disclosure of their personal data since 2007 and 2014, respectively. In 2023, the FCC adopted updated data breach notification rules with additional protections for consumers.

Did you know?

While updates to modernize the FCC's Breach Notification Rules were adopted in 2023, the amendments to the Code of Federal Regulations (CFR) statutes were delayed indefinitely and are therefore not enforced. **Radar® Privacy represents the currently enforced rules and continues to monitor for an FCC announcement in the Federal Register regarding the amendments to the CFR statutes**.

FCC Breach Notification Rules

The FCC's Breach Notification Rules reflect that telecommunications companies may be particularly vulnerable to attacks as they collect large amounts of personal data and they are considered a critical service.

Of particular note in the FCC's Breach Notification Rules are:

- **Regulated Data:** The Breach Notification Rules only regulate customer proprietary network information (CPNI) and do not extend to other elements of personal or sensitive personal information.

- **Regulator Notification Requirements:** Telecommunications carriers and TRS providers are required to notify the U.S. Secret Service (USSS), as well as the Federal Bureau of Investigation (FBI), after reasonable determination of a breach involving their customers' proprietary network information. TRS providers must also notify the Disability Rights Office of the Consumer and Governmental Affairs Bureau.
- **Customer Notification Waiting Period:** A mandatory seven-business-day waiting period is required between the notification to the USSS and FBI and the notification to affected customers or disclosure to the public.
- **Mandatory Harm-based Notifications:** Notification is required to customers whose CPNI was involved in a breach regardless of whether the breach is likely to cause harm.
- **Breach Definition:** The breach threshold is contingent on intentional conduct. Unintentional access to, use, or disclosure of CPNI is not considered a breach.

© Copyright RADAR, LLC. All Rights Reserved. 0724

Entities Covered Under the FCC's Breach Notification Rules

The FCC's Breach Notification Rules cover providers of telecommunications and telecommunications relay services (TRS).

- **Telecommunications carriers:** Any provider of telecommunications services, except aggregators of telecommunications services, including entities that provide interconnected Voice over Internet Protocol (VoIP) service.
- **Telecommunications relay services (TRS) providers:** Entities that allow individuals who are deaf, hard of hearing, deaf-blind, or who have speech disabilities to communicate using voice communication services in an equivalent manner as a hearing individual, including entities that provide point-to-point service.

FCC Notification Obligation Intelligence with Radar® Privacy

Telecommunications companies must find new and effective ways to thrive in a highly dynamic regulatory environment. They are not only critical services, but protectors of vast amounts of PII, as well as data that could lead to the disclosure of highly sensitive customer information.

There is little room for error when it comes to protecting their customers' privacy. Telecommunications carriers and TRS providers must have a defined process for identifying, documenting, and notifying regulators of data breaches.

The FCC understands that breaches are inevitable in the telecommunications industry. Their expectation is that your organization is deeply prepared with consistent processes for documenting, assessing, and notifying—before a breach occurs. The first time you trial a playbook should never be in the midst of a live remediation effort.

Automation to Simplify FCC Compliance

Radar® Privacy operationalizes and simplifies compliance with the FCC's Breach Notification Rules by applying **assessment automation and intelligent notification guidance to eliminate the subjectivity and inconsistency inherent in deciding whether breaches are reportable—to federal agencies and customers alike**.

The FCC Breach Notification Rules are unique in that: only CPNI is regulated and the rules do not extend to other elements of personal or sensitive personal information; a breach refers to the intentional access, use, or disclosure of CPNI; and the rules do not provide a harm standard as a condition of notification in the event of a breach.

The FCC module in Radar® Privacy is uniquely configured to address these specific assessment needs. The intelligent decision automation provided by the module ensures consistent and timely incident assessments to decrease time to resolution and ensure your organization can satisfy the FCC's unique breach notification requirements for providers of telecommunications and telecommunications relay services.

Avoid costly penalties and fines—and an erosion of trust—with the FCC module in Radar® Privacy.

INFO@RADARFIRST.COM | 1.844.737.3778

Schedule a Demo >

RadarFirst

Learn more at radarfirst.com

RadarFirst offers enterprise risk solutions to automate intelligent decisions for state, federal, international, and industry-specific regulations. Our patented assessment technology enables organizations to act quickly to determine obligations with evolving legal, contractual, and regulatory requirements. With RadarFirst, organizations can confidently navigate complex privacy and compliance reporting with consistent, documented decision-making.

© Copyright RADAR, LLC. All Rights Reserved. 0724