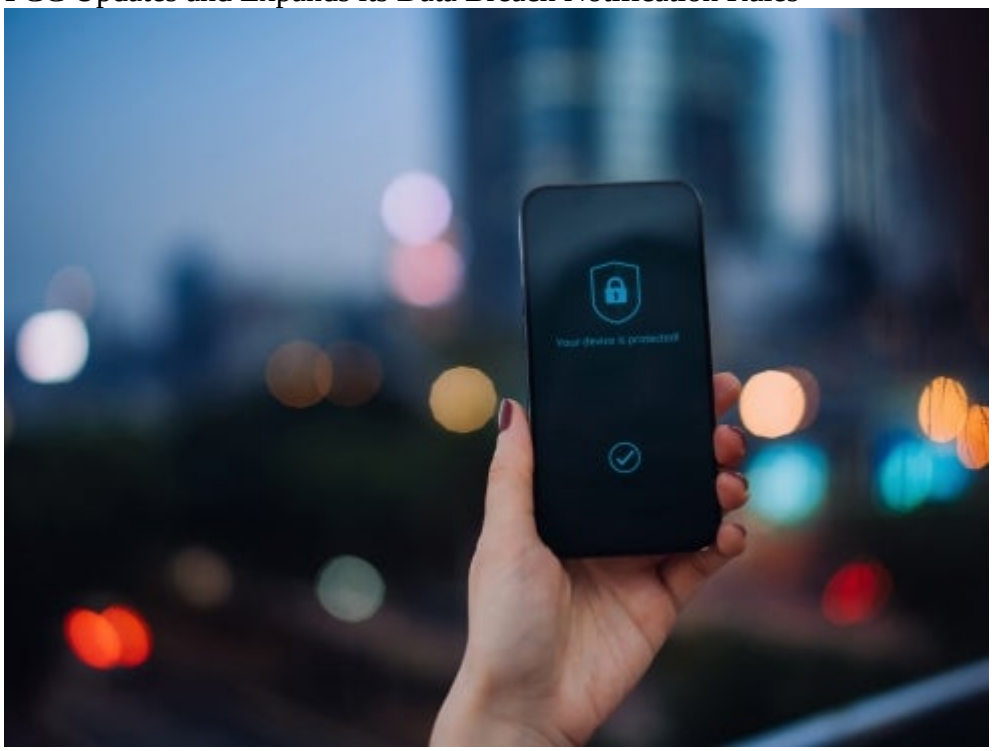
Updates
December 21, 2023
FCC Updates and Expands its Data Breach Notification Rules



In a politically divided 3-2 vote, the FCC updated its data breach notification rules, which had been in effect since before the release of the first iPhone.

Background

The new, consumer-friendly rules apply to telecommunications services providers and Voice over Internet Protocol (VoIP) providers (carriers), as well as telecommunications relay services (TRS) providers, which are entities that allow customers with hearing or speech disabilities to place and receive calls. The rules (1) expand the scope of breach notifications to include all of a customer's personally identifiable information (PII), defined as "information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual"; (2) expand the definition of "breach" to include inadvertent PII disclosures by carriers and TRS providers; and (3) place new notification obligations on carriers and TRS providers. The rules also eliminate the requirement to notify customers when the carrier or TRS provider can "reasonably determine that no harm to customers is reasonably likely to occur," as well as the mandatory seven-day waiting period before carriers could notify customers of a breach.

Rules for the Digital Age

Inclusion of PII

FCC Chairwoman Jessica Rosenworcel heralded the new rules as the emergence from analog into the digital age with a stated goal of encouraging carriers to adopt stronger data security practices, including encryption, for all PII. The FCC's prior rules had limited breach notification requirements to disclosures of Customer Proprietary Network Information (CPNI), a well-established regulatory definition that includes phone numbers; frequency, duration, and timing of calls made by its customers; and any services purchased by its customers. But with the

inclusion of all PII, breach notification now extends to a subscriber's name, address, and telephone number, regardless of whether such information is publicly available.

Inadvertent Disclosures

The FCC's prior rules were primarily concerned with intentional "pretexting" (e.g., phishing) by malicious third parties seeking to gain unauthorized access to customer information. The new rules eliminate this intent limitation, expanding notification requirements to include inadvertent disclosure or access by other carriers, TRS providers, and their employees and agents, unless "such information is not used improperly or further disclosed." This exception aims to strike a balance between incentivizing stronger data security practices while reducing unnecessary notifications that could desensitize customers to the importance of notifications.

Notification to the FCC

While notifying the FCC is an additional obligation (the prior rules only required notification to federal law enforcement), the new rules mitigate this burden by requiring that the FCC coordinate with law enforcement to adapt the existing reporting systems for simultaneous notification to both the FCC and law enforcement. The FCC also created two notification regimes tailored to the severity of the breach. For breaches that affect 500 or more customers (or where the number of customers affected is not known), carriers and TRS providers must "file individual, per-breach notifications as soon as practicable, but no later than seven business days, after reasonable determination of a breach." For smaller, less risky breaches, carriers and TRS providers may provide notice in summary form on an annual basis.

Notification to Customers

Consistent with the exception to the inadvertent disclosure rule, the FCC adopted a "harm-based notification trigger" in which notification is not required where "a carrier can reasonably determine that no harm to customers is reasonably likely to occur." Carriers and TRS providers are required to consider a number of factors in reaching such a conclusion, including the sensitivity of the information, nature and duration of the breach, whether the information is encrypted (and the encryption key remains secure), any carrier or TRS provider mitigations taken, and the intentionality of the unauthorized access.

Mandatory Waiting Period Eliminated

The FCC removed the mandatory seven-day waiting period between when a carrier or TRS provider notifies law enforcement and when they may notify affected customers. Instead, following notification to law enforcement, the FCC now requires notification to affected customers "without unreasonable delay" but "in no case more than 30 days following discovery" of the breach. However, law enforcement may still request an initial delay of up to 30 days to safeguard potentially confidential national security and criminal investigations.

Trouble Ahead?

These rules are not the FCC's first foray into data breach notification requirements. In November 2016, the FCC adopted a robust set of data privacy and breach notification rules (the 2016 Data Privacy Order), in which the FCC required carriers to notify affected customers, the FCC, and law enforcement of a breach unless the carrier "determined that no harm to customers was reasonably likely to occur." However, in early 2017, shortly after election of a Republican majority in the House and Senate and the inauguration of President Trump, Congress and the White House acted together to overturn those rules under the Congressional Review Act (CRA), prohibiting the FCC from readopting the 2016 Data Privacy Order or a substantially similar order unless Congress expressly re-authorizes such delegated authority. It was actually only the second successful use of the

CRA since 2001, when President George W. Bush and the 107th Congress acted together to overturn a Clinton administration workplace ergonomics rule adopted by the Occupational Safety and Health Administration (OSHA). Once the 2016 Data Privacy Order was overturned, the Trump administration and the 115th Congress relied on the CRA 15 more times to overturn Obama administration regulations.

In this order, the FCC has concluded that the CRA only prohibits it from reissuing the 2016 Data Privacy Order "in whole, or in substantially the same form." In other words, the FCC believes it retains authority to adopt individual rules or some combination of rules from the 2016 Data Privacy Order—a reading that has drawn the ire of the FCC's Republican commissioners and some Republican senators on procedural grounds. Given this political dispute, this order may face court challenges centered on the lasting effects of the CRA on an agency's rulemaking authority.

Authors

Explore more in

Technology Transactions & Privacy Law Privacy & Security Advertising, Marketing & Promotions Communications

Related insights

Update

Illinois Pay Transparency Requirements Arrive

Update

Trump’s FDA and USDA: Five Key Issues To Watch in 2025