LATHAM&WATKINS

Client Alert Commentary

Latham & Watkins Privacy & Cyber Practice

January 3, 2024 | Number 3201

FCC Expands Data Breach Notification Rules

The amended rules follow the Biden Administration's "whole of government" approach to maximizing notifications to executive agencies of cybersecurity events.

On December 21, 2023, a divided Federal Communications Commission (FCC or the Commission) released a Report and Order updating its data breach reporting rules for certain telecommunications providers. The updated rules require that providers of telecommunications services, interconnected Voice over Internet Protocol (VoIP), and telecommunications relay services (TRS) adequately safeguard sensitive customer information and report data breaches to the Commission. The rules will also likely apply to providers of broadband Internet access services when the Commission completes its recently initiated rulemaking proposing to reclassify broadband as a telecommunications service covered by the data breach rules.

In a 3-2 vote, the Commission expanded the breach notification regulations to cover breaches that involve personally identifiable information (PII), in addition to customer proprietary network information (CPNI). Both PII and CPNI are now considered "covered data" under the applicable rules. Further, the rules now extend to inadvertent disclosures of covered data, along with intentional disclosures without authorization. Upon determining that a breach has occurred, carriers must notify the Commission via the FCC's existing central reporting facility in addition to notifying the FBI and the Secret Service.

Federal agency notifications must be submitted "as soon as practicable," but no later than seven business days after determination of a breach. The Commission emphasized that, depending on the circumstances, a "failure to swiftly report breaches may ... be untimely and unreasonable, even if within the seven business day timeline."[1] Carriers must also notify affected data subjects in a timely manner — eliminating the mandatory seven-day waiting period after notifying law enforcement that previously applied before a carrier could begin notifying customers.

Additional Changes Promote Carrier Accountability

The Report and Order institutes several other changes aimed at increasing carriers' accountability for breaches, including:

- **Elimination of intent requirement.** The Commission hopes that eliminating the intent requirement and including inadvertent disclosures "will encourage telecommunications carriers to adopt stronger data security practices, and will help federal agencies identify and address systemic network vulnerabilities."[2] The Commission also aims to "reduce ambiguity regarding whether reporting a breach is necessary."[3]

- **Harm-based triggers for customer notification.** In an effort to mitigate concerns about potentially excessive notice due to the expanded coverage of inadvertent disclosures, the Commission clarified that customer notice is not required if the carrier can "reasonably determine that no harm to customers is reasonably likely to occur."[4] Importantly, because the Report and Order adopts a rebuttable presumption of harm, customer notification *is* required if a carrier cannot make such a determination.

  The concept of "harm" is broad and goes beyond financial harm to include, among others, identity theft, potential for blackmail, reputational harm, and mental pain and emotional distress. When there is "no definitive evidence of actual harm," the Commission provides five factors to consider when determining if harm is reasonably likely to occur: (1) the sensitivity of the breached information, (2) the nature and duration of the breach, (3) mitigation efforts, (4) intentionality, and (5) encryption.[5]

  Although the Commission did not characterize encryption as dispositive to the harm-based analysis, it noted that encryption "significantly" reduces "the risk of actual harm" and that encryption may be a safe harbor under which customer notification is not required in certain circumstances.[6]

- **Harm-based and affected customer thresholds for federal reporting.** For any breaches that "affect 500 or more customers, or for which a carrier cannot determine how many customers are affected," a carrier must file the federal agency notification "as soon as practicable, but no later than seven business days, after reasonable determination of a breach."[7] The same standard applies for breaches affecting fewer than 500 customers "unless the carrier can reasonably determine" that the breach "is not reasonably likely to harm these customers."[8] If the carrier can make such a determination, then such breaches can instead be reported on an annual summary filed via the central reporting facility.

In dissent, the two Republican commissioners argued that the Commission was prohibited from adopting these changes, asserting that they are substantially similar to a 2016 Privacy Order that was overturned by a 2017 Congressional Review Act resolution. The dissenting commissioners also objected on the ground that including PII expands the coverage of the regulations beyond the FCC's jurisdiction, which they contend is limited to CPNI.

Criticism Over Potential Duplication of CIRCIA

The FCC received substantial criticism of the amendments during the comment period. Commenters questioned the necessity of the proposed changes given that multiple data breach reporting regimes either already exist or will be implemented soon. Commenters also argued that PII, which the FCC added to the definition of "covered data," is already subject to extensive regulation under more than 50 state breach notification laws and several federal regimes. Trade groups also expressed concern that the FCC's expanded rules may duplicate the upcoming Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) breach notification regulation.

Much more will be known about the CIRCIA approach in the next few months. CIRCIA directs the Cybersecurity and Infrastructure Security Agency (CISA) to publish a notice of proposed rulemaking by March 15, 2024, with a final rule due 18 months later. CISA must propose and adopt rules for covered entities to report cyber incidents within 72 hours and ransomware payments within 24 hours.

To prepare for these efforts, the Department of Homeland Security released a report that will likely guide future federal disclosure requirements. The report inventories 45 effective and seven proposed federal cyber incident reporting requirements across 22 agencies. Along with providing a model reporting form, the report recommends ways for the federal government to harmonize these requirements, including by

establishing “a model definition for reportable cyber incidents” and “model timelines and triggers for reporting.” [9]

Concerns over future conflicts between the FCC and CISA rules could prove unwarranted, since CIRCIA exempts “covered entities from the reporting requirements to CISA if the entity is required to report substantially similar information to another federal agency within a substantially similar timeframe and CISA and the Federal agency have an agreement and information sharing mechanism in place.”[10]

Given CISA’s ambitious efforts to design a single portal for all federal government incident reporting, these updated FCC rules may be modified again to accommodate the CIRCIA regulatory timeframes. In the meantime, stakeholders should keep watch for the Wireline Competition Bureau’s announcement of the rules’ final approval by the Office of Management and Budget and their effective dates.

If you have questions about this Client Alert, please contact one of the authors listed below or the Latham lawyer with whom you normally consult:

Jennifer C. Archie
jennifer.archie@lw.com
+1.202.637.2205
Washington, D.C.

Matthew A. Brill
matthew.brill@lw.com
+1.202.637.1095
Washington, D.C.

Gabriela Aroca Montaner
gabriela.arocamontaner@lw.com
+1.202.637.2200
Washington, D.C.

Chad Kenney
chad.kenney@lw.com
+1.202.350.5388
Washington, D.C.

Molly Whitman
Knowledge Management Lawyer
molly.whitman@lw.com
+1.213.891.8156
Los Angeles

You Might Also Be Interested In

FTC Refines Road Map for AI Enforcement

New York Bolsters Cybersecurity Requirements

SEC Outlines 2024 Examination Priorities

New Cyber Incident Reporting Requirements on the Horizon in the US

Endnotes

[1] *Data Breach Reporting Requirements*, WC Docket No. 22-21, Report & Order, FCC 22-111, 23, para. 38 (2023) (*Report and Order*).

[2] *Id.* at 13, para. 21.

[3] *Id.* at 14, para. 23.

[4] *Id.* at 15, para. 24.

[5] *Id.* at 32, para. 54; *see id.* at 32-36, paras. 54-58.

[6] *Id.* at 35-36, para. 58.

[7] *Id.* at 20, para. 31.

[8] *Id.*

[9] Department of Homeland Security, *Harmonization of Cyber Incident Reporting to the Federal Government* iii (2023).

[10] *Id.* at 12-13.