Cooley

FCC Enforcement Actions Pose New Risks for Vendors to Telecom Companies

September 23, 2024

Last week, the Federal Communications Commission (FCC) released a $13 million settlement with AT&T that concluded an investigation into a third-party data breach that exposed AT&T customer data. This is the latest in a series of investigations the FCC has conducted into licensees and their relationship with third-party vendors. In many of those cases, the FCC has held the licensee liable for actions taken (or not taken) by a third party.

The case stemmed from a 2023 data breach involving one of AT&T's marketing vendors. AT&T shared customer information with the unidentified vendor between 2015 and 2017 for purposes of creating and hosting personalized video content for AT&T customers. Pursuant to agreements between AT&T and the vendor, the vendor should have destroyed or deleted this information years ago. However, the vendor failed to do so, and AT&T did not identify this failure, despite reviewing and assessing the vendor between 2016 and 2020. When threat actors later breached the vendor's cloud environment in January 2023, they were able to exfiltrate sensitive information relating to nearly nine million AT&T customers.

Although the breach occurred at the vendor rather than at AT&T, the FCC held AT&T liable for not ensuring that the vendor adequately protected AT&T customer information and returned/destroyed that information as required under applicable agreements. The FCC alleged that AT&T's failures constituted a violation of its rules requiring FCC licensees to protect customers' personal information. In addition to paying the $13 million civil penalty, the settlement requires AT&T to implement a range of improvements to its privacy and data security practices – including a detailed vendor oversight program.

This action shows the FCC's keen interest in data breaches involving cloud service providers that work with telecommunications companies. For instance, the FCC cited studies identifying the high percentages of data breaches involving cloud-based service providers due to such service providers' poor security and data management practices. The settlement also follows previous actions involving AI-generated deepfake voice messages and robocalls in which the FCC used subpoenas to investigate violations of its rules. We expect the FCC to continue to use its authority to compel production of information and testimony through subpoenas.

These FCC actions have implications for licensees and their vendors. Third parties should evaluate how they provide services to companies regulated by the FCC. First and foremost, responding to an FCC third-party subpoena puts a spotlight on the contractual relationship and ongoing cooperation of the parties. In addition, indemnification, limitation of liability, warranties, confidentiality, force majeure, insurance provisions and the interplay of such clauses will become increasingly important as the FCC continues to take action against licensees for third-party failures. Finally, onerous vendor oversight terms – like those that AT&T agreed to – may become standard contractual terms for FCC-regulated companies, altering the relationship between vendors and licensees.

Licensees and vendors should account for these possibilities when negotiating contracts. It's also critical to have experienced counsel to help respond to subpoenas issued by the FCC, whether or not the vendor is the primary subject of the FCC's investigation.

assistance of artificial intelligence (AI) in accordance with our AI Principles, may be considered Attorney Advertising and is subject to our legal notices.

Key Contacts

Henry Wendel **Washington, DC**	**hwendel@cooley.com** **+1 202 776 2943**
J.G. Harrington Washington, DC	jgharrington@cooley.com +1 202 776 2818
Ronald W. Del Sesto Washington, DC	rdelsesto@cooley.com +1 202 728 7128
Tamar E. Finn Washington, DC	tfinn@cooley.com +1 202 728 7129
Christopher Suhler Colorado	csuhler@cooley.com +1 720 566 4376