FCC NEWS from the Federal Communications Commission

Media Contact:
MediaRelations@fcc.gov

For Immediate Release

FCC ANNOUNCES $13 MILLION SETTLEMENT WITH AT&T RESOLVING VENDOR CLOUD BREACH INVESTIGATION

Company Must Implement Expansive Improvements to Cloud and Supply Chain Security to Protect Consumer Data and Privacy

WASHINGTON, September 17, 2024—The Federal Communications Commission today announced a $13 million settlement with AT&T to resolve an Enforcement Bureau investigation into the company's supply chain integrity and whether it failed to protect the information of AT&T customers in connection with a data breach of a vendor's cloud environment. AT&T used the vendor to generate and host personalized video content, including billing and marketing videos, for AT&T customers. Under AT&T's contracts, the vendor should have destroyed or returned AT&T customer information when no longer necessary to fulfill contractual obligations, which ended years before the breach occurred. AT&T failed to ensure the vendor: (1) adequately protected the customer information, and (2) returned or destroyed it as required by contract. In January 2023, threat actors exfiltrated AT&T customer information from the vendor's cloud environment. The investigation examined whether AT&T failed to protect customer information and engaged in unreasonable privacy, cybersecurity, and vendor management practices in connection with the breach. To resolve the investigation, AT&T entered into a Consent Decree that also commits to strengthening its data governance practices to increase its supply chain integrity and ensure appropriate processes and procedures are incorporated into AT&T's business practices in the handling of sensitive data to protect consumers against the harmful effects of similar vendor data breaches in the future.

"The Communications Act makes clear that carriers have a duty to protect the privacy and security of consumer data, and that responsibility takes on new meaning for digital age data breaches," **said FCC Chairwoman Jessica Rosenworcel.** "Carriers must take additional precautions given their access to sensitive information, and we will remain vigilant in ensuring that's the case no matter which provider a customer chooses."

"As high-value targets, communications service providers have an obligation to reduce the attack surface and entry points that threat actors seek to exploit in order to access sensitive customer data," **said Enforcement Bureau Chief Loyaan A. Egal, who also serves as Chair of the FCC's Privacy and Data Protection Task Force.** "Today's announcement should send a strong message that the Enforcement Bureau will not hesitate to take action against service providers that choose to put their customers' data in the cloud, share that data with their vendors, and then fail to be responsible custodians of that data."

The growing nexus between privacy, cybersecurity, and supply chain risks associated with cloud security and vendor security, coupled with vendor oversight vulnerabilities across industry, make the terms of this Consent Decree especially timely and necessary. The Communications Act of

1934 and the Commission's rules require telecommunications companies to protect customers' personal information and take all necessary steps to safeguard customer data. These requirements include responsibility for cloud and vendor security, as well as an obligation to engage in reasonable practices as they relate to cloud security, data retention and disposal, and vendor oversight. Further, the Act makes clear that carriers are responsible for the acts of their agents and contractors. Companies that choose to share their customers' data with vendors must act as responsible stewards and hold their vendors responsible for protecting that data as required by the Communications Act.

The Consent Decree's expansive consumer privacy and data protection terms or "Consumer Privacy Upgrades" include requirements to:

- Enhance tracking of customer data as part of a data inventory program;
- Require vendors to adhere to retention and disposal obligations;
- Implement multifaceted vendor controls and oversight;
- Implement a comprehensive Information Security Program to include broad customer data protections; and
- Conduct annual compliance audits.

Implementing the terms of this Consent Decree will require AT&T to make significant investments in and prioritize the safeguarding of customers' information shared with third parties. Given AT&T's size, number of customers, and extensive use of vendors, this will likely require expenditures far greater than the civil penalty herein. The Commission will hold AT&T accountable for making these mandatory changes to its data protection practices as required to comply with this Consent Decree and the Communications Act going forward.

In 2023, FCC Chairwoman Rosenworcel established the Privacy and Data Protection Task Force, an FCC staff working group focused on coordinating across the agency on the rulemaking, enforcement, and public awareness needs in the privacy and data protection sectors, including data breaches (such as those involving telecommunications providers) and vulnerabilities in regulated communications providers' privacy and cybersecurity practices. Thanks to the work of the Task Force and a renewed focus on consumer protections more broadly under Chairwoman Rosenworcel, the Commission secured similar "Consumer Privacy Upgrades" covering beneficial data protection, cybersecurity, and consumer privacy terms with the largest wireless carriers, including today's AT&T settlement and a July 2024 settlement with Verizon on behalf of TracFone. More information on the Task Force is available at: https://www.fcc.gov/privacy-and-data-protection-task-force.

The Consent Decree is available at: https://www.fcc.gov/document/fcc-eb-settles-att-vendor-cloud-breach.

###

Media Relations: (202) 418-0500 / ASL: (844) 432-2275 / 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).