FCC NEWS from the Federal Communications Commission

Media Contact:
MediaRelations@fcc.gov

For Immediate Release

FCC REACHES MULTI-MILLION DOLLAR SETTLEMENT OF INVESTIGATIONS INTO T-MOBILE DATA BREACHES WITH SIGNIFICANT IMPROVEMENTS TO COMPANY'S CYBERSECURITY

All Major Wireless Carriers Now Required to Make Investments to Protect Consumer Data and Privacy

WASHINGTON, September 30, 2024—The Federal Communications Commission today announced a groundbreaking data protection and cybersecurity settlement with T-Mobile to resolve the Enforcement Bureau's investigations into significant data breaches that impacted millions of U.S. consumers. To settle the investigations, T-Mobile has agreed to important forward-looking commitments to address foundational security flaws, work to improve cyber hygiene, and adopt robust modern architectures, like zero trust and phishing-resistant multi-factor authentication. The Commission believes that implementation of these commitments, backed by a $15.75 million cybersecurity investment by the company as required by the settlement, will serve as a model for the mobile telecommunications industry. As part of the settlement, the company will also pay a $15.75 million civil penalty to the U.S. Treasury.

"Today's mobile networks are top targets for cybercriminals," **said FCC Chairwoman Jessica Rosenworcel**. "Consumers' data is too important and much too sensitive to receive anything less than the best cybersecurity protections. We will continue to send a strong message to providers entrusted with this delicate information that they need to beef up their systems or there will be consequences."

Today's settlement resolves multiple cybersecurity breach investigations. The Bureau had opened cases into cybersecurity incidents involving T-Mobile in 2021, 2022, and 2023. These investigations developed evidence that the breaches that occurred, which affected millions of cell phone customers, were varied in their nature, exploitations, and apparent methods of attack. Additional details about the incidents are available in the settlement.

"The wide-ranging terms set forth in today's settlement are a significant step forward in protecting the networks that house the sensitive data of millions of customers nationwide," **said Loyaan A. Egal, Chief of the Enforcement Bureau and Chair of the Privacy and Data Protection Task Force**. "With companies like T-Mobile and other telecom service providers operating in a space where national security and consumer protection interests overlap, we are focused on ensuring critical technical changes are made to telecommunications networks to improve our national cybersecurity posture and help prevent future compromises of Americans' sensitive data. We will continue to hold T-Mobile accountable for implementing these commitments."

Today's settlement includes enforceable commitments by T-Mobile including:

- **Corporate Governance** – T-Mobile's Chief Information Security Officer will give regular reports to the board concerning T-Mobile's cybersecurity posture and business risks posed by cybersecurity. This is a foundational requirement for all well-governed companies. Corporate boards need both visibility and cybersecurity domain experience in order to effectively govern. This commitment ensures that the board's visibility into cybersecurity is a key priority going forward.
- **Modern Zero-Trust Architecture** – T-Mobile has agreed to move toward a modern zero trust architecture and segment its networks. This is one of the most important changes organizations can make to improve their security posture.
- **Robust Identity and Access Management** – T-Mobile has committed to broad adoption of multi-factor authentication methods within its network. This is a critical step in securing critical infrastructure, such as our telecommunications networks. Abuse of authentication methods, for example through the leakage, theft, or deliberate sale of credentials, is the number one way that breaches and ransomware attacks begin. Consistent application of best practice identity and access methods will do more to improve a cybersecurity posture than almost any other single change.

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 all of the largest wireless carriers, including today's T-Mobile settlement, a September 2024 settlement with AT&T, 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.

###

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