FCC NEWS from the Federal Communications Commission

Media Contact:
MediaRelations@fcc.gov

For Immediate Release

TRACFONE TO PAY $16 MILLION TO SETTLE FCC INVESTIGATIONS INTO CARRIER'S DATA PROTECTION AND CYBERSECURITY PRACTICES

Settlement Includes Comprehensive Terms Addressing API and Data Security Vulnerabilities Following Enforcement Bureau Investigations of Three Data Breaches

WASHINGTON, July 22, 2024—The Federal Communications Commission today announced a settlement with TracFone Wireless to resolve investigations into whether TracFone failed to reasonably protect its customers' information from unauthorized access in connection with three data breaches.

The underlying data breaches involved exploitation of application programming interfaces (APIs). APIs allow different computer programs or components to communicate with one another. Among other things, numerous APIs can be leveraged to access customer information from websites. The settlement, formally called a Consent Decree, includes terms aimed at strengthening TracFone's API security. This is critical because APIs are ubiquitous, and thus are a common attack vector for threat actors.

"Carriers—and the customer information they have access to—are prime targets for threat actors. The Commission takes matters of consumer privacy, data protection, and cybersecurity seriously, including in the context of emerging security issues. The Enforcement Bureau's investigations and resulting Consent Decree make clear that API security is paramount and should be on the radar of all carriers," said Loyaan A. Egal, Chief of the Enforcement Bureau and chair of the Privacy and Data Protection Task Force.

TracFone is a telecommunications carrier that offers services through multiple brands, such as Straight Talk, Total by Verizon Wireless, and Walmart Family Mobile. TracFone is a wholly-owned subsidiary of Verizon Communications, which acquired the company in November 2021. Between January 2021 and January 2023, TracFone experienced three data breaches. The breaches resulted in the unauthorized access to and exposure of customers' proprietary information (PI), including certain customer proprietary network information (known as CPNI) and personally identifiable information (known as PII), as well as numerous unauthorized port-outs.

The failure to reasonably secure customers' proprietary information violates a carrier's duty under Section 222 of the Communications Act and also constitutes an unjust and unreasonable practice in violation of Section 201 of the Act. It is also a violation of Section 222 of the Communications Act to impermissibly use, disclose, or permit access to individually identifiable CPNI without customer approval. The Commission has made clear that it expects telecommunications carriers to take "every reasonable precaution" to protect their customers' proprietary or personal information. The Commission has also adopted rules that require carriers to take reasonable measures to discover, report, and protect against attempts to access CPNI without authorization.

In addition to a $16 million civil penalty, the Consent Decree includes:

- a mandated information security program, with novel provisions to reduce API vulnerabilities in ways consistent with widely-accepted standards, like those identified by the National Institute of Standards and Technology (NIST) and the Open Worldwide Application Security Project (OWASP);
- Subscriber Identity Module (SIM) change and port-out protections;
- annual assessments, including by independent third parties, of its information security program; and
- privacy and security awareness training to employees and certain third parties.

Today's action follows the Commission's issuance of nearly $200 million in fines against the nation's largest wireless carriers for illegally sharing access to customers' location information without consent and without taking reasonable measures to protect that sensitive information against unauthorized disclosure.

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. More information on the Task Force is available at: https://www.fcc.gov/privacy-and-data-protection-task-force.

Today's settlement, formally called a Consent Decree, is available at: https://www.fcc.gov/document/eb-settles-tracfone-following-three-data-breaches.

###

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