FCC Enforcement Monitor

By Scott R. Flick, Jessica Nyman and Joseph Cohen

Headlines:

- *FCC Proposes $25,000 Fine Against Individual for Operating a Pirate Radio Station*
- *FCC Admonishes Wireless Carrier for Data Breach*
- *Telecommunications Relay Service Providers Agree to $9.1 Million Settlement*

Pirate Radio Operator Faces $25,000 Proposed Fine After Flaunting Multiple FCC Warnings

After issuing multiple warnings, the FCC proposed a $25,000 fine against a New Jersey man for operating an unlicensed radio station. Section 301 of the Communications Act prohibits any person from operating any apparatus for the transmission of energy or communications or signals by radio within the United States without FCC authorization.

In October 2015, the licensee of an FM translator station in Jersey City complained to the FCC that an unauthorized station was causing co-channel interference. FCC agents verified the complaint and issued a Notice of Unlicensed Operation ("NOUO") to the owner of the apartment building where the unlicensed station was operating. The unauthorized broadcast subsequently stopped. However, in May 2016, the FCC received another complaint and found that the unlicensed station was operating again. FCC agents issued a second NOUO, this time to both the individual operating the pirate station and the building owner. The individual contacted the FCC in June 2016, at which time he was warned he could face additional enforcement action if unlicensed operations continued.

Despite that admonition, FCC agents found the individual again engaged in unlicensed operation in August 2016, this time at a different site. The FCC issued another NOUO, but later that month found the individual operating without a license again, this time at yet another site.

FCC guidelines set a base fine for unauthorized operation of $10,000 for each violation or each day of a continuing violation. The FCC may adjust the fine upward or downward after taking into account the particular facts of each case. Here, the FCC found that a "significant upward adjustment was warranted" due to the individual's disregard of multiple warnings. As a result, the FCC proposed a $20,000 base fine—

$10,000 for the May 2016 operations and another $10,000 for the August 2016 operations—and applied a $5,000 upward adjustment, for a total proposed fine of $25,000.

Hack of Wireless Carrier Leads to Admonishment by FCC

The FCC admonished a national wireless phone carrier for a 2015 data breach in which a third party gained unauthorized access to personal information collected by the carrier to run credit checks on customers.

Section 222(a) of the Communications Act requires telecommunications carriers to "protect the confidentiality of proprietary information of, and relating to . . . customers." It also requires carriers to "take every reasonable precaution" to protect personal customer information. Section 201(b) of the Act requires practices related to interstate or foreign telecommunications to be "just and reasonable."

In September 2015, the carrier discovered a data breach that affected 15 million customers, and compromised data such as names, social security numbers, addresses, and other identifying information. The FCC began investigating the breach in October 2015 and learned that the carrier relied on a vendor to keep personal customer information safe. The FCC found that the vendor failed to use reasonable measures to protect the carrier's personal customer information. Among other deficiencies, the vendor failed to patch known, critical vulnerabilities on the servers where it processed the carrier's sensitive customer information, failed to protect database passwords, and failed to monitor for unauthorized access or suspicious activity. Further, the FCC found that the carrier did not reasonably oversee the vendor and ignored several "red flags." For example, the FCC concluded that the carrier (1) did not take meaningful action to review or improve the vendor's security practices following a similar 2013 data breach, (2) lacked general knowledge regarding the vendor's systems, and (3) consistently failed to follow up with the vendor regarding its compliance with contractual security requirements.

The FCC therefore determined that the carrier's data security practices were unjust and unreasonable and issued an order admonishing the carrier. The FCC explained in its order that the carrier was ultimately responsible for the vendor's failings, because "while [providers] can outsource functions, they cannot transfer accountability."

Although the FCC found that a monetary forfeiture against the carrier was warranted and would have been consistent with past precedent, Section 503(b)(6)(B) of the Act limited it to admonishment because the violations took place more than one year prior to the issuance of the FCC's order. Section 503(b)(6)(B) states that the FCC cannot issue a forfeiture for a violation that occurs more than one year prior to the issuance of a notice of forfeiture or notice of apparent liability. The FCC stated that it was nevertheless sending a "strong signal" to carriers that they are responsible for the actions of third parties acting on their behalf.

FCC Resolves Investigation of Improper Billing and Other Violations by Two TRS Providers

The FCC entered into a Consent Decree with two Internet telecommunications relay service ("TRS") providers, one in California and one in Florida, to resolve an investigation into the providers' failure to properly verify customers, submission of improper bills for reimbursement, and other violations.

The TRS Fund reimburses telephone providers that provide services to consumers with hearing and speech disabilities. Internet-based TRS ("iTRS") allows such consumers to communicate with hearing persons via the Internet. There are currently three forms of iTRS: (1) Video Relay Service ("VRS"); Internet Protocol Relay Service; and (3) Internet Protocol Captioned Telephone Service.

Section 64.615(a)(5) of the FCC's Rules requires that for some forms of TRS providers must verify the registration information of each TRS user before providing service. Section 64.604(c)(5)(iii)(D)(1) requires that TRS providers submit "true and accurate data" to the TRS Fund Administrator.

In December 2015, the FCC adopted a Forfeiture Order, affirming an $11.9 million fine against the California provider for failing to implement a reasonable verification process and improperly billing the TRS Fund for calls associated with unverified users. Later that month, the FCC issued Letters of Inquiry to both companies regarding their compliance with iTRS numbering obligations and VRS requirements.

In February 2017, the parent company of the Florida provider acquired the California provider. Immediately following the acquisition, the FCC released a Consent Decree terminating its investigations into the two providers. As part of the Consent Decree, the General Counsel of the parent company will serve as a Compliance Officer for both providers and oversee regulatory compliance efforts, including the implementation of a five-year compliance plan.

Under the compliance plan, the providers must, among other things, develop and implement measures to ensure the accuracy of call data submitted to the TRS Fund Administrator, measures to ensure customer records are accurate, and a compliance training program. The companies must also file compliance reports with the FCC every year for the next five years. Lastly, in addition to reimbursing the TRS Fund a total of $6,116,579, the companies must pay a civil penalty of $3 million to the U.S. Treasury.

If you have any questions about the content of this Advisory, please contact the Pillsbury attorney with whom you regularly work, or the authors of this Advisory.

Scott R. Flick (bio)
Washington, DC
+1.202.663.8167
scott.flick@pillsburylaw.com

Jessica Nyman (bio)
Washington, DC
+1.202.663.8810
jessica.nyman@pillsburylaw.com

Joseph A. Cohen (bio)
Washington DC
+1.202.663.8172
joseph.cohen@pillsburylaw.com