FCC Proposes $10 Million in Fines for Privacy and Data Security Violations

October 28, 2014

On October 24, the FCC, over the dissent of its two Republican commissioners, issued a Notice of Apparent Liability (NAL) proposing a fine of $10 million to Lifeline eligible telecommunications carriers ("ETCs") TerraCom, Inc. and YourTel America, Inc. for violations of laws protecting "phone customers' personal information."

This is the agency's first data security case and the largest privacy action in the Commission's history. See News Release. Friday's decision follows through on numerous public statements made by FCC Enforcement Bureau Chief Travis LeBlanc indicating that privacy and security is a high enforcement priority for the Commission and that the agency would begin to use a Communications Act provision barring unjust and unreasonable practices as a privacy and security enforcement tool.

According to the NAL, the Enforcement Bureau investigation found that both TerraCom and YourTel "collected names, addresses, Social Security numbers, driver's licenses and other proprietary information" gathered through the Lifeline eligibility approval process "and stored them on unprotected Internet servers that anyone in the world could access with a search engine and basic manipulation." The NAL states that the TerraCom and YourTel violations exposed more than 300,000 customers' personal information to unauthorized access as well as heightened risk of fraud and identity theft. CPNI Violation. The NAL first alleges that the companies failed to properly protect the confidentiality of consumers' proprietary information collected from applicants for wireless and wired Lifeline services in violation of Section 222(a) of the Communications Act, which requires that carriers protect the confidentiality of the "proprietary information" of their customers. The FCC proposes a forfeiture of $8.5 million for this violation based on precedent for base forfeitures of $29,000 for previous CPNI violations. Applying the base forfeitures to the alleged over 300,000 violations would have resulted in a proposed penalty of close to $9 billion, but the FCC settled on $8.5 million as "sufficient."

Unjust and Unreasonable Practices. The NAL next alleges several violations of Section 201(b) of the Communications Act, which prohibits unjust and unreasonable practices, but only proposes a penalty for one such violation. The NAL proposes a $1.5 million penalty against the companies for making false representations in their website privacy policies regarding protecting customers' sensitive personal information. The FCC alleges that the companies' failure to follow their own privacy policies was an unjust and unreasonable practice. This forfeiture is based on precedent for a $40,000 base forfeiture for Section 201(b) violations related to deceptive marketing to consumers.

Further, the NAL alleges that by failing to employ reasonable data security practices (such as password protection or encryption) and failing to notify all potentially affected customers of the security breach, the companies apparently violated Section 201(b). However, the agency declined to propose a forfeiture for those two alleged violations because this is the first case in which it makes

such findings. The NAL states that carriers are now on notice regarding these potential violations.

The Commission's use of its authority to police "unjust and unreasonable" practices by telecommunications providers appears to represent a significant expansion of the Commission's enforcement authority over privacy-related matters and appears to mirror the Federal Trade Commission's privacy and data security actions under a similar statutory provision in the Federal Trade Commission Act Section 5 barring unfair and deceptive trade practices. The expansion of authority is the reason that Commissioners Pai (R) and O'Reilly (R) dissented. Both Commissioners contended that the FCC had not given fair notice of what data security practices are required. Commissioner O'Reilly also questioned the majority's interpretation of the CPNI provisions of Section 222. While the $10 million proposed penalty is the largest privacy action in the Commission's history and its first foray into data security enforcement, it is not likely to be its last. We expect that the FCC will continue to investigate and take enforcement action against lax data security and other practices that compromise the privacy of consumers' personal information.

In light of the FCC's action, all carriers, including especially Lifeline providers, should review their security and privacy practices related to customer eligibility documentation and other personal information, as well as their privacy statements and CPNI policies to ensure that consumer data is adequately safeguarded in a manner that comports not only with the FCC's CPNI rules but also with federal and state privacy frameworks that will inform the Commission's determination of what is "unjust and unreasonable" in this area.