AT&T To Pay $25 Million to Resolve FCC Data Breach Claims

April 12, 2015

On April 8, 2015, the Federal Communications Commission (FCC) Enforcement Bureau announced that AT&T has agreed to a $25 million consent decree to resolve an FCC investigation into alleged consumer privacy violations at AT&T call centers in Mexico, Columbia, and the Philippines. According to the FCC, AT&T violated Section 222 of the Communications Act (the "Act") by failing to reasonably secure its customers' personal information, including customers' names and at least the last four digits of their Social Security numbers, as well as account-related data known as customer proprietary network information (CPNI). The agency further alleged that AT&T's data security practices at the three call centers were unjust and unreasonable in violation of Section 201 of the Act. The settlement is the FCC's largest data security enforcement action to date.

The FCC launched its investigation into AT&T in May 2014 after AT&T reported a data breach to the Commission's CPNI Data Breach Portal. The breach occurred between November 2013 and April 2014 at a third-party call center facility in Mexico under contract with AT&T. According to the FCC, while AT&T did not operate the call center where the breach occurred, AT&T maintained and operated the systems that certain employees at the Mexico call center used to access AT&T customer records, and such systems were governed by AT&T's data security measures. The FCC asserted that AT&T's measures failed to prevent or timely detect the breach that lasted 168 days and resulted in the unauthorized access of more than 68,000 customer accounts. The employees as issue sold the data from the customer accounts to an unauthorized third-party who used the information to submit up to 290,000 handset unlock requests through AT&T's website as part of what appeared to be a fraudulent used or stolen phone trafficking operation. AT&T terminated its relationship with the Mexico call center in September 2014.

In March 2015, AT&T disclosed to the FCC that it was investigating separate data breaches at call centers in Columbia and the Philippines, in which call center employees accessed account data for at least 211,000 customer accounts to obtain unlock codes for AT&T mobile phones. The unauthorized access exposed certain customer CPNI including bill amount and rate plan information, though AT&T's investigation found no evidence that the CPNI was used or sold to third-parties.

To read more about the terms of the FCC consent decree with AT&T, visit our sister blog here.

The consent decree with AT&T comes six months after the FCC's first data security enforcement action. In that case, the FCC issued a Notice of Apparent Liability (or NAL) seeking to impose $10 million in fines against TerraCom, Inc. and YourTel America, Inc. for allegedly violating Sections 222 and 201 of the Act by maintaining the sensitive personal data of 300,000 consumers on unencrypted Internet servers. These actions underscore the FCC's heightened and growing emphasis on consumer privacy and data security, areas that traditionally have been the focus of the Federal Trade Commission, which has brought more than 50 privacy and data security actions across a

number of industries during the past 10 years.