FCC Action Against AT&T Reflects Regulator's Increasing Focus on Privacy and Data Security

In the wake of the Federal Communications Commission's ("FCC's") first-ever foray last October into fining companies over data security practices, the agency's Enforcement Bureau Chief, Travis LeBlanc, asserted that the agency "will not tolerate" conduct that, in the agency's view, "puts American consumers at risk of financial fraud and identity theft." Thus, said LeBlanc at the time, while that action was the agency's first in the data security space, "it will not be the last."

Now, six months later, the FCC has followed through on that warning with a $25 million settlement with AT&T. This fine, the largest for privacy or data security violations in the agency's history, confirms that it intends to aggressively claim authority over privacy and data security practices. Nor does this new assertion of authority appear to be focused solely on companies traditionally thought to be within FCC jurisdiction. With the agency's recent classification of broadband Internet access as a telecommunications service through its Open Internet Order and other signals of intent to expand the reach of communications laws (including those relating to privacy), a number of new practices are now apparently within the FCC's sights.

The events leading to the $25 million settlement with AT&T began with an alleged series of data security breaches at AT&T international call-centers in Mexico, Columbia, and the Philippines. From 2013 to 2014, approximately 43 call center employees allegedly accessed customer information without authorization and then provided it to third parties. These third parties in turn used the information to request the consumer device codes necessary to unlock thousands of stolen and secondary market mobile phones. The employees' actions, according to the FCC, resulted in the unauthorized disclosure of almost 280,000 U.S. customers' names and full or partial social security numbers, as well as unauthorized access to account-related data known as "customer proprietary network information" ("CPNI").

The FCC's settlement with AT&T resolved its investigation into whether, through these alleged data security breaches, AT&T violated Sections 201(b) and 222 of the Communications Act of 1934. Section 201(b) proscribes certain charges, practices, classifications, and regulations that are "unjust or unreasonable." Section 222 and regulations the FCC has adopted thereunder place certain restrictions on how telecommunications firms may "use, disclose, or permit access to" CPNI.

Under the terms of the consent decree, AT&T agreed to pay a civil penalty of $25 million, the largest amount obtained by the FCC in a privacy or data security enforcement action to date. AT&T also agreed to designate a compliance officer and to develop and implement a data security compliance plan, which is to include a risk assessment, a documented information security program, an employee training program, and other measures. In addition, AT&T promised to notify certain customers of unauthorized access to their information and to provide them with a year of complimentary credit monitoring.

The FCC's action against AT&T highlights the agency's increasing focus on privacy and data security issues. To date, the federal agency claiming the lead in this space has been the Federal Trade Commission ("FTC"), which, under its statutory framework to monitor and bring enforcement actions to prevent unfair or deceptive trade practices, has entered into a series of consent settlements with companies whose cybersecurity practices allegedly have been inconsistent with those companies' stated protection practices or, in a few cases, have been so inadequate as to allegedly constitute an "unfair" practice in the FTC's eyes. For its part, within the last year, the FCC has initiated fines or obtained settlements in five major cases over alleged privacy or data security violations, including, as discussed above, a data security-based action against TerraCom and YourTel America in October 2014 for allegedly storing names, addresses, driver's licenses, social security numbers, and other customer information on Internet servers without password protection or

encryption. With its most recent settlement in the AT&T matter, the FCC has left no doubt that its emerging interest in data security matters matches or even exceeds the FTC's.

Indeed, the FCC's settlement with AT&T contains negotiated compliance requirements over and above those typically obtained by the FTC in its own data security settlements. For instance, whereas AT&T agreed to pay a $25 million civil penalty to the FCC, the FTC typically cannot obtain civil penalties in its data security settlements because it lacks civil penalty power under Section 5 of the FTC Act, the statute the agency normally relies upon in such cases. AT&T also agreed to notify certain customers of unauthorized access to their information and provide complimentary credit monitoring services, a provision not typically found in FTC data security settlements. And while FTC settlements often include an agreement by the settling company to designate an employee or employees to coordinate the required information security program, AT&T's settlement with the FCC additionally specifies that the compliance officer administering the program have knowledge of the communication laws and information security principles and practices necessary to implement the requirements of the consent decree, as well as that either the compliance officer or his or her subordinates be "privacy certified by an industry certifying organization."

In short, with its AT&T settlement, the FCC has entered the fray alongside the FTC, Securities and Exchange Commission and other agencies as an aggressive actor in the privacy and data security space. That being so, all companies that collect or use consumer information in ways that could potentially implicate FCC jurisdiction would do well to proactively review their policies and practices and assess any risks of FCC scrutiny.

For more information regarding the settlement between AT&T and the FCC or to discuss data security practices generally, please feel free to contact Jim DeGraw, Seth Harrington, David McIntosh, Doug Meal, Mark Szpak, Michelle Visser, David Cohen, or another member of Ropes & Gray's leading privacy & data security team.

James S. DeGraw
Seth C. Harrington
David McIntosh
Douglas H. Meal
Mark P. Szpak
Michelle Visser
David T. Cohen