Implications of FCC's Record $25M Data Breach Settlement with AT&T

The Federal Communications Commission ("FCC") announced today that AT&T Services, Inc. ("AT&T") agreed to a $25 million settlement to resolve the Commission's investigation into whether AT&T failed to protect the confidentiality of its customers' proprietary network information. The penalty is the FCC's largest data security enforcement action to date.

According to the consent decree, breached information included customers' names, at least four digits of customers' Social Security Numbers, and other sensitive, account-related information. The FCC stated that the breaches occurred when employees at AT&T's call centers in Mexico, Colombia, and the Philippines accessed more than 280,000 customer accounts without authorization and then sold that data to third parties.

Failure to Take "Every Reasonable Precaution." Chastising AT&T for "lax data security practices," FCC Chairman Tom Wheeler stated in a press release that "the Commission will exercise its full authority against companies that fail to safeguard the personal information of their customers." The FCC stated that it expects telecommunications carriers to "take 'every reasonable precaution' to protect their customers' data" and to promptly notify law enforcement upon becoming aware of a breach.

Untimely Reporting. The Commission requires telecommunications carriers to notify law enforcement "[a]s soon as practicable, in no event later than seven (7) business days, after reasonable determination of the breach."[1] According to the consent decree, AT&T commenced its investigation into the breach on April 3, 2014, and immediately became aware that the breached data contained sensitive customer billing and proprietary network information. AT&T began its forensic investigation upon receiving the hard drives from the computers involved in the breach on April 22, 2014. But it was not until May 20, 2014—33 business days after learning of the breach—that AT&T notified the United States Secret Service and the Federal Bureau of Investigation. That did not sit well with the FCC. In the Order accompanying the consent decree, Travis LeBlanc, Chief of the Commission's Enforcement Bureau, wrote that "the laws that require prompt disclosure of data breaches to law enforcement authorities, and subsequently to consumers, aid in the pursuit and apprehension of bad actors and provide valuable information that helps affected customers be proactive in protecting themselves in the aftermath of a data breach."

Terms of the Agreement. To settle the matter, AT&T paid a civil penalty of $25,000,000 and must develop and implement a comprehensive compliance plan. AT&T also must conduct a privacy risk assessment, implement an information security program, prepare a compliance manual, and provide employees with regular training on privacy law and the company's privacy policies. Furthermore, AT&T must, within 30 days, appoint a senior compliance manager who is privacy certified. Unsurprisingly, the settlement also requires that AT&T notify all affected customers and provide them with free credit monitoring services.

What This Means. There are two key takeaways from this settlement. First, companies cannot discount the risk of the "insider threat." A company may spend millions on cybersecurity

[1] 47 C.F.R. § 64.2011(b).

defenses designed to secure the company from outside threats only to fall victim to the nefarious (or even unwitting) actions of a single employee. Companies should design their information security programs accordingly. Second, as this settlement illustrates, government regulators are increasingly willing to hold companies accountable for not only their conduct leading up to a breach, but also their conduct following the breach. We will never know what the FCC's response to this matter would have been had AT&T promptly notified law enforcement, but it is hard to imagine a settlement amount of this magnitude. This settlement also makes clear the importance of understanding and complying with applicable notification laws and regulations. Determining when to report a data breach to law enforcement is not an easy decision, but failing to do so timely is getting significantly more costly.