

Memorandum

FCC Fines AT&T \$25 Million In Biggest Settlement Yet Over Consumer Privacy Breaches

April 15, 2015

Introduction

On April 8, 2015, the Federal Communications Commission (“FCC”) announced a \$25 million settlement—the FCC’s largest privacy and data security enforcement action to date—with the telecommunications carrier AT&T Services, Inc. (“AT&T”) for a series of alleged privacy breaches from 2013 through 2014 that may have compromised almost 280,000 customers’ proprietary information.¹ In the Consent Decree in *In the Matter of AT&T Services, Inc.*, the FCC alleged that AT&T violated Sections 201(b) and 222(c) of the Communications Act of 1934, as amended (the “Communications Act”), and Sections 64.2010(a) and 64.2011(b) of the FCC’s rules.²

Section 201(b) of the Communications Act prohibits “unjust or unreasonable” practices when providing interstate or foreign communication service by wire or radio.³ Section 222(c) of the Communications Act permits a telecommunications carrier to use, disclose, or access individually identifiable customer proprietary network information (“CPNI”) only in order to provide telecommunications services or other necessary services.⁴ To further protect CPNI, the FCC also promulgated Section 64.2010(a) of its rules, which requires telecommunications carriers to “take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI,” and Section 64.2011(b), which requires telecommunications carriers to notify law enforcement of a breach of its customers’ CPNI “[a]s soon as practicable, and in no

¹ See Federal Communications Commission, “[AT&T To Pay \\$25M To Settle Investigation Into Three Data Breaches](#)” (April 8, 2015).

² *In the Matter of AT&T Services, Inc.*, File No. EB-TCD-14-00016243, Consent Decree at 1 (Apr. 8, 2015).

³ 47 U.S.C. § 201(b).

⁴ 47 U.S.C. § 222(c).

event later than seven (7) business days, after reasonable determination of the breach.”⁵

In May 2014, the FCC’s Enforcement Bureau (the “Bureau”) launched its investigation of potential data breaches at AT&T’s call center in Mexico that occurred between November 2013 and April 2014. During its investigation, the Bureau also learned of additional data breaches at AT&T’s call centers in Colombia and the Philippines. Employees at the call centers allegedly accessed customers’ accounts and CPNI without authorization and obtained a total of almost 280,000 U.S. customers’ names, full or partial Social Security numbers, and other personal information. According to the Bureau’s findings, account information was sometimes provided to third parties, who used the information to submit online requests for cellular handset unlock codes.⁶

Without admitting that it violated the Communications Act or Sections 64.2010(a) and 64.2011(b) of the FCC’s Rules, AT&T agreed to pay a \$25 million civil penalty. The company must also provide written notice to all customers affected by the breaches in Colombia and the Philippines and offer one year of credit monitoring services.⁷ In addition, AT&T agreed to:

- appoint a compliance officer;
- conduct a privacy risk assessment;
- establish an information security program to protect CPNI information;
- distribute a compliance manual;
- train employee on compliance with Section 222, the FCC’s rules, and the company’s privacy policies; and
- file periodic compliance reports with the FCC.

Implications of the Action

The FCC’s current action against AT&T comes in the wake of five major enforcement actions against other companies over consumer privacy and data security issues and reflects a heightened focus by regulators on these issues.⁸ As observed by FCC Chairman Tom Wheeler, the recent enforcement actions demonstrate that “the Commission will exercise its full authority against companies that fail to safeguard the personal

⁵ 47 C.F.R. §§ 64.2010, 64.2011.

⁶ See Federal Communications Commission, *supra* note 1.

⁷ *In the Matter of AT&T Services, Inc.*, Consent Decree at 9, *supra* note 2.

⁸ In May 2014, the FCC announced a \$2.9 million planned fine against Dialing Services, LLC due to its alleged violation of FCC rules that protect consumers from harassing, intrusive, and unwanted robocalls to mobile devices. In the same month, Sprint Corporation entered in a \$7.5 million settlement for its alleged failure to honor consumers’ do-not-call or do-not-text requests. Verizon settled with the FCC in September 2014 for the company’s marketing practices. In October 2014, the FCC announced a \$10 million planned fine against TerraCom, Inc. and YourTel America, Inc. for their alleged failure to protect customers’ personal information. Federal Communications Commission, *supra* note 1.

information of their customers.”⁹

The FCC’s settlement with AT&T is the most recent reminder of the ever increasing importance for companies to “properly secure customer data, promptly notify customers when their personal data has been breached, and put in place robust internal processes to prevent against future breaches.”¹⁰ It also exemplifies the importance of a company’s vendor chain in protecting customer data. It is critical for companies to have robust procedures in place to ensure that third-party vendors meet specified privacy standards and to properly draft termination provisions in third-party agreements.

If you have any questions or would like additional information, please do not hesitate to contact **Yafit Cohn** at +1-212-455-3815 or yafit.cohn@stblaw.com; **Monica Chan** at +1-212-455-2816 or monica.chan@stblaw.com; or any other member of the Firm’s Public Company Advisory Practice, Litigation Practice, or Data Privacy and Cybersecurity Practice.

The contents of this publication are for informational purposes only. Neither this publication nor the lawyers who authored it are rendering legal or other professional advice or opinions on specific facts or matters, nor does the distribution of this publication to any person constitute the establishment of an attorney-client relationship. Simpson Thacher & Bartlett LLP assumes no liability in connection with the use of this publication. Please contact your relationship partner if we can be of assistance regarding these important developments. The names and office locations of all of our partners, as well as our recent memoranda, can be obtained from our website, www.simpsonthacher.com.

⁹ *Id.*

¹⁰ *Id.*



UNITED STATES

New York
425 Lexington Avenue
New York, NY 10017
+1-212-455-2000

Houston
2 Houston Center
909 Fannin Street
Houston, TX 77010
+1-713-821-5650

Los Angeles
1999 Avenue of the Stars
Los Angeles, CA 90067
+1-310-407-7500

Palo Alto
2475 Hanover Street
Palo Alto, CA 94304
+1-650-251-5000

Washington, D.C.
1155 F Street, N.W.
Washington, D.C. 20004
+1-202-636-5500

EUROPE

London
CityPoint
One Ropemaker Street
London EC2Y 9HU
England
+44-(0)20-7275-6500

ASIA

Beijing
3919 China World Tower
1 Jian Guo Men Wai Avenue
Beijing 100004
China
+86-10-5965-2999

Hong Kong
ICBC Tower
3 Garden Road, Central
Hong Kong
+852-2514-7600

Seoul
West Tower, Mirae Asset Center 1
26 Eulji-ro 5-gil, Jung-gu
Seoul 100-210
Korea
+82-2-6030-3800

Tokyo
Ark Hills Sengokuyama Mori
Tower
9-10, Roppongi 1-Chome
Minato-Ku, Tokyo 106-0032
Japan
+81-3-5562-6200

SOUTH AMERICA

São Paulo
Av. Presidente Juscelino
Kubitschek, 1455
São Paulo, SP 04543-011
Brazil
+55-11-3546-1000