Before the
Federal Communications Commission
Washington, DC 20554

In the Matter of	)	
	)	
AT&T Services, Inc.	)	File No.: EB-TCD-14-00016243
	)	Acct. No.: 201532170010
	)	FRN: 0005193701
	)	
	)	

ORDER

Adopted: April 8, 2015 **Released: April 8, 2015**

By the Chief, Enforcement Bureau:

1. The Enforcement Bureau (Bureau) of the Federal Communications Commission (Commission) has entered into a Consent Decree to resolve its investigation into whether AT&T Services, Inc. (AT&T or Company) failed to properly protect the confidentiality of almost 280,000 customers' proprietary information, including sensitive personal information such as 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), in connection with data breaches at AT&T call centers in Mexico, Columbia, and the Philippines. At least two employees believed to have engaged in the unauthorized access confessed that they sold the information obtained from the breaches to a third party, known to them as "El Pelon." The breaches resulted in the personal information of 51,422 AT&T customers' information being used to place 290,803 handset unlock requests through AT&T's online customer unlock request portal. The investigation also examined whether AT&T promptly notified law enforcement authorities of the security breaches involving its customers' CPNI.

2. The failure to reasonably secure customers' proprietary information violates a carrier's statutory duty under the Communications Act to protect that information, and also constitutes an unjust and unreasonable practice in violation of the Act. These laws ensure that consumers can trust that carriers have taken appropriate steps to ensure that unauthorized persons are not accessing, viewing or misusing their personal information. The Commission has made clear that it expects telecommunications carriers such as AT&T to take "every reasonable precaution" to protect their customers' data, and that it is committed to protecting the personal information of American consumers from misappropriation, breach, and unlawful disclosure. In addition, 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 consumers be proactive in protecting themselves in the aftermath of a data breach. To settle this matter, AT&T will pay a civil penalty of $25,000,000 and develop and implement a compliance plan to ensure appropriate processes and procedures are incorporated into AT&T's business practices to protect consumers against similar data breaches in the future. In particular, AT&T will be required to improve its privacy and data security practices by appointing a senior compliance manager who is privacy certified, conducting a privacy risk assessment, implementing an information security program, preparing an appropriate compliance manual, and regularly training employees on the company's privacy policies and the applicable privacy legal authorities.

3. After reviewing the terms of the Consent Decree and evaluating the facts before us, we find that the public interest would be served by adopting the Consent Decree and terminating the referenced investigation regarding AT&T's compliance with 201(b) and 222 of the Communications Act

of 1934, as amended (Communications Act or Act),[1] and Sections 64.2010(a) and 64.2011(b) of the Commission's Rules[2] in connection with a data breach.

4. In the absence of material new evidence relating to this matter, we conclude that our investigation raises no substantial or material questions of fact as to whether AT&T possesses the basic qualifications, including those related to character, to hold or obtain any Commission license or authorization.

5. Accordingly, **IT IS ORDERED** that, pursuant to Section 4(i) of the Act[3] and the authority delegated by Sections 0.111 and 0.311 of the Rules[4] the attached Consent Decree **IS ADOPTED** and its terms incorporated by reference.

6. **IT IS FURTHER ORDERED** that the above-captioned matter **IS TERMINATED.**

7. **IT IS FURTHER ORDERED** that a copy of this Order and Consent Decree shall be sent by first class mail and certified mail, return receipt requested, to Mr. James Talbot and Ms. Jackie Flemming, AT&T Services, 1120 20th St. NW, Suite 1000, Washington, DC 20036.

FEDERAL COMMUNICATIONS COMMISSION

Travis LeBlanc
Chief
Enforcement Bureau

[1] *See* 47 U.S.C. §§ 201, 222.

[2] *See* 47 C.F.R. §§ 64.2010(a), 64.2011(b).

[3] 47 U.S.C. § 154(i).

[4] 47 C.F.R §§ 0.111, 0.311.

Before the
Federal Communications Commission
Washington, DC 20554

In the Matter of	)	
	)	
AT&T Services, Inc.	)	File No.: EB-TCD-14-00016243
	)	Acct. No.: 201532170010
	)	FRN: 0005193701
	)	
	)	

CONSENT DECREE

1. The Enforcement Bureau of the Federal Communications Commission and AT&T Services, Inc. (AT&T or Company), by their authorized representatives, hereby enter into this Consent Decree for the purpose of terminating the Enforcement Bureau's investigation into whether AT&T violated Sections 201(b) and 222[1] of the Communications Act of 1934, as amended (Communications Act or Act),[2] and Sections 64.2010(a) and 64.2011(b) of the Commission's Rules[3] in connection with a data breach.

I. DEFINITIONS

2. For the purposes of this Consent Decree, the following definitions shall apply:

(a) "Act" means the Communications Act of 1934, as amended.

(b) "Adopting Order" means an order of the Bureau adopting the terms of this Consent Decree without change, addition, deletion, or modification.

(c) "Affected Customer" means any AT&T customer whose account was accessed without the customer's authorization by an employee of a call center in Colombia or the Philippines for the purpose of obtaining unlock codes.

(d) "AT&T" or "Company" means AT&T Services, Inc., and its affiliates, subsidiaries, predecessors-in-interest, and successors-in-interest.

(e) "Bureau" means the Enforcement Bureau of the Federal Communications Commission.

(f) "Commission" and "FCC" mean the Federal Communications Commission and all of its bureaus and offices.

(g) "Call Center" means call centers operated by AT&T Mobility or its contractor(s) that provide mobility customer service or wireless sales service for AT&T Mobility consumer customers.

(h) "Communications Laws" means, collectively, the Act, the Rules, and the published and promulgated orders and decisions of the Commission to which AT&T is subject by virtue of its business activities.

[1] 47 U.S.C. §§ 201(b), 222.

[2] 47 U.S.C. § 151 *et seq.*

[3] 47 C.F.R. §§ 64.2010(a), 64.2011(b).

(i) "Compliance Plan" means the compliance obligations, program, and procedures described in this Consent Decree at paragraph 18.

(j) "Covered Employees" means all employees and agents of AT&T who perform or directly supervise, oversee, or manage the performance of duties that involve access to, use, or disclosure of Personal Information or Customer Proprietary Network Information at Call Centers managed and operated by AT&T Mobility. Covered Employees do not include Covered Vendor Employees.

(k) "Covered Vendor Employees" means all employees and agents of Vendors who perform or directly supervise, oversee, or manage the performance of duties that involve access to, use, or disclosure of Personal Information or CPNI at Vendor Call Centers that provide customer service and wireless sales services for AT&T Mobility customers.

(l) "Customer Proprietary Network Information" and "CPNI" shall have the meaning set forth at Section 222(h)(1) of the Act.

(m) "CPNI Rules" means the rules set forth at 47 C.F.R. § 64.2001 *et seq.* and any amendments or additions to those rules subsequent to the Effective Date.

(n) "Data Breach" means access to a customer's account without authorization for the purpose of obtaining the customer's name, cellular telephone number, and last four digits of the customer's Social Security number to be used to obtain an unlock code.

(o) "Effective Date" means the date by which both the Bureau and AT&T have signed the Consent Decree.

(p) "Investigation" means the investigation commenced by the Bureau in EB-TCD-14-00016243.

(q) "Operating Procedures" means the standard internal operating procedures and compliance policies established by AT&T to implement the Compliance Plan.

(r) "Parties" means AT&T and the Bureau, each of which is a "Party."

(s) "Personal Information" means either of the following: (1) an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted: (A) Social Security number; (B) driver's license number or other government-issued identification card number; or (C) account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account; or (2) a user name or email address, in combination with a password or security question and answer that would permit access to an online account.

(t) "Rules" means the Commission's regulations, found in Title 47 of the Code of Federal Regulations.

(u) "Vendor" means a third-party that operates and/or manages a Call Center on behalf of AT&T Mobility and provides customer service and wireless sales services for AT&T Mobility consumer customers.

II. BACKGROUND

3. Section 222(c) of the Act, entitled "Confidentiality of Customer Proprietary Network Information," restricts carriers' use and disclosure of CPNI.[4] Section 222(c)(1) only permits a carrier to disclose, permit access to, or use a customer's individually identifiable CPNI to provide telecommunications services, or other services "necessary to, or used in," the carrier's telecommunications service, unless otherwise authorized by the customer or required by law.[5]

4. The Commission has adopted rules implementing Section 222(c)'s protections of CPNI. Section 64.2010(a) of the Commission's Rules requires that "carriers must take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI."[6] Section 64.2011(b) requires a telecommunications carrier to notify designated law enforcement authorities of a "breach" of its customers' CPNI "[a]s soon as practicable, in no event later than seven (7) business days, after reasonable determination of the breach . . . ."[7] A "breach" occurs "when a person, without authorization or exceeding authorization, has intentionally gained access to, used, or disclosed CPNI."[8] A telecommunications carrier must provide notice of a breach to the United States Secret Service (USSS) and the Federal Bureau of Investigation (FBI) through an online portal.[9]

5. Section 201(b) of the Act states, in part, that "[a]ll charges, practices, classifications, and regulations for and in connection with [interstate or foreign] communication service [by wire or radio], shall be just and reasonable, and any such charge, practice, classification, or regulation that is unjust or unreasonable is declared to be unlawful."[10] The Notice of Apparent Liability in *TerraCom* states that Section 201(b) applies to carriers' practices for protecting customers' PII and CPNI.[11]

6. AT&T is a telecommunications carrier that provides mobile voice and data services to customers throughout the United States, with its principal place of business in Dallas, Texas.[12] AT&T is the second largest wireless carrier in the United States, with over 100 million subscribers, earning $126.4 billion in revenue in 2012 and $128.8 billion in 2013.[13]

7. In May 2014, the Enforcement Bureau (Bureau) began investigating an internal Data Breach that occurred between November 2013 and April 2014 at a facility in Mexico under contract with

[4] *See* 47 U.S.C. § 222(c).

[5] *Id.* at § 222(c)(1).

[6] 47 C.F.R. § 64.2010(a).

[7] 47 C.F.R. § 64.2011(b).

[8] 47 C.F.R. § 64.2011(e).

[9] 47 C.F.R. § 64.2011(b). The Commission maintains a link to the portal at http://www.fcc.gov/eb/cpni. Telecommunications carriers are required to report CPNI data breaches via the online portal accessible through that site. The data reported through the FCC portal is collected by U.S. Secret Service and the Federal Bureau of Investigation.

[10] 47 U.S.C. § 201(b).

[11] *TerraCom, Inc. and YourTel America, Inc.*, Notice of Apparent Liability for Forfeiture, 29 FCC Rcd 13325, 13335–36, paras. 31–32 (2014).

[12] AT&T is an interexchange carrier (499 Filer ID Number: 806172). New Cingular Wireless Services, Inc. CONSOLIDATED, is listed as providing Cellular/PCS/SMR services and doing business as AT&T Mobility (499 Filer ID Number: 821002). AT&T's principal place of business is located at 208 S. Akard Street, Dallas, TX 75202. Randall Stephenson is the Chief Executive Officer.

[13] *See AT&T's 2013 Annual Report*, http://www.att.com/Investor/ATT_Annual/2013/financial_highlights.html (lasted visited Jan. 20, 2015).

AT&T (the April 2014 Breach). The Bureau's investigation[14] into the April 2014 Breach was based on reports submitted by AT&T to the Commission's CPNI Data Breach Portal[15] and publicly available information.[16] AT&T informed the Bureau that it discovered that three employees of an AT&T Vendor that provided Spanish-language customer support services from an inbound Call Center located in Mexico (Mexico Call Center), had used login credentials to access customer accounts to obtain customer information—specifically, names and the last four digits of customers' Social Security numbers—that could then be used to submit online requests for cellular handset unlock codes.[17]

8. AT&T maintained and operated the systems the Mexico Call Center employees used to access AT&T customer records. These systems were governed by AT&T's data security measures.[18] In this case, those measures failed to prevent or timely detect a large and ongoing Data Breach. The April 2014 Breach lasted 168 days (from November 4, 2013, until April 21, 2014). During this period, the three Mexico Call Center employees accessed 68,701 customers' accounts, without authorization to obtain the above-referenced information required for unlock codes, which appeared on the same account page as these customers' CPNI.[19] Beginning in December 2013, more than 11,000 customer accounts were accessed each month until March 2014.[20] AT&T also determined that the personal information of 51,422 of these customers was used to place 290,803 handset unlock requests through AT&T's online customer unlock request portal.[21] Although CPNI appeared on the same page as the information required for unlock codes, AT&T found no evidence that the Mexico Call Center employees used or disclosed CPNI in connection with the data breach. In December 2012, an AT&T employee became suspicious that an employee at the Mexico Call Center was possibly providing customer information to unauthorized persons.[22] The Mexico Call Center employee was terminated by the Mexico Call Center for accessing customer accounts without leaving account notations.[23] In January 2013, AT&T discovered information

[14] The Bureau issued two Letters of Inquiry (LOIs) to AT&T, seeking information about the April 2014 Breach, other reported security breaches, and AT&T's data security practices generally. *See* Letter from Richard A. Hindman, Chief, Telecommunications Consumers Division, FCC Enforcement Bureau, to Jackie Flemming, AT&T Services, Inc. (June 30, 2014) (on file in EB-TCD-14-00016243); *see also* Letter from Richard A. Hindman, Chief, Telecommunications Consumers Division, FCC Enforcement Bureau, to Jackie Flemming, AT&T Services, Inc. (November 7, 2014) (on file in EB-TCD-14-00016243). AT&T responded to the LOI on July 29, 2014. *See* Letter from James Talbot, General Attorney, AT&T, to Richard A. Hindman, Chief, Telecommunications Consumers Division, FCC Enforcement Bureau (July 29, 2014) (on file in EB-TCD-14-00016243) (LOI Response). AT&T submitted a response to the Supplemental LOI on December 8, 2014. *See* Letter from James Talbot, General Attorney, AT&T, to Richard A. Hindman, Chief, Telecommunications Consumers Division, FCC Enforcement Bureau (Dec. 8, 2014) (on file in EB-TCD-14-00016243) (Supplemental LOI Response).

[15] *See supra* note 9.

[16] AT&T reported the April 2014 Breach to the California Attorney General. *See* Submitted Breach Notification Sample, State of California Department of Justice, Office of the Attorney General, http://oag.ca.gov/ecrime/databreach/reports/sb24-45415 (lasted visited Dec. 19, 2014); *see also* Martyn Williams, *AT&T says customer data accessed to unlock smartphones*, ITWORLD (June 12, 2014), http://www.itworld.com/article/2695622/security/at-t-says-customer-data-accessed-to-unlock-smartphones.html (last visited Jan. 29, 2015).

[17] *See* LOI Response at 19.

[18] *See* Supplemental LOI Response at 6.

[19] *See* LOI Response at 5–6, 20.

[20] *See* LOI Response at 5.

[21] *See* LOI Response at 21.

[22] *See* Supplemental LOI Response at 8–9.

[23] *See* Supplemental LOI at 9.

that another at the Mexico Call Center may have engaged in suspicious activities suggesting access to accounts for an improper purpose.[24] This employee left the Mexico Call Center voluntarily prior to the completion of AT&T's investigation.[25] AT&T did not classify the 2012 and 2013 incidents as CPNI breaches at the time that they occurred because AT&T did not conclude that the breaches included use or disclosure of CPNI. Following the April 2014 Breach, however, AT&T re-examined these incidents and reported them to the USSS and FBI via the CPNI breach reporting portal in September 2014.[26]

9. AT&T commenced its investigation of the April 2014 Breach on April 3, 2014, and notified members of its senior management of the investigation on April 4, 2014.[27] According to AT&T, "it was quickly apparent that the incident potentially involved a high volume of customer account access."[28] AT&T was aware from the outset of its investigation that the customer database that was accessed to perpetrate the suspected breach contained billing information and other CPNI.[29] On April 8, 2014, the Mexico Call Center, in consultation with AT&T, interviewed one of the employees suspected of engaging in the breach, concluded that the employee presented an "evasive attitude" during the interview, and, after conducting a polygraph examination of the employee, severed him from his job functions and began the process to terminate his employment.[30] By April 22, 2014, AT&T had received the imaged hard drives from computers believed to have been involved in the breach, and began its forensic analysis shortly thereafter.[31] On May 20, 2014, AT&T notified the USSS and the FBI of the incident.[32] As noted above, Section 64.2011(b) requires a carrier to notify law enforcement of a CPNI breach "[a]s soon as practicable, and in no event later than seven (7) business days, after reasonable determination of the breach . . . ."[33] AT&T reported completing notification to customers affected by the breach on July 3, 2014.[34]

10. AT&T informed the Bureau that it terminated its use of the Mexico Call Center on September 28, 2014.[35]

11. In March 2015, AT&T disclosed to the Bureau that it was investigating additional potential Data Breaches in Colombia and the Philippines. AT&T informed the Bureau that its

[24] *Id.*

[25] *Id.*

[26] *See* Supplemental LOI Response at 8–9. In December 2014, AT&T identified additional customer accounts that appeared to have been accessed by these employees in 2012. AT&T treated these incidents as CPNI breaches and reported them via the online portal. *See* Supplemental LOI Response at 9–10.

[27] *See* LOI Response at 6.

[28] LOI Response at 15.

[29] *See* LOI Response at 1.

[30] *See* LOI Response at 17.

[31] *See* LOI Response at 17.

[32] *See* LOI Response at 20.

[33] 47 C.F.R. § 64.2011(b).

[34] *See* LOI Response at 7. AT&T determined that approximately 156 prepaid customers, however, did not have valid physical addresses or email addresses and those customers were notified via SMS message on July 10, 2014.

[35] *See* Letter from James Talbot, General Attorney, AT&T, to Richard A. Hindman, Chief, Telecommunications Consumers Division, FCC Enforcement Bureau (Jan. 23, 2015) (on file in EB-TCD-14-00016243); *see also* e-mail from James Talbot, Attorney, AT&T Services, Inc., to Rosemary Cabral, Attorney-Advisor, Telecommunications Consumers Division, FCC Enforcement Bureau (Jan. 27, 2015, 15:42 EDT).

investigation was ongoing but that thus far it had discovered that call center employees in Bogota, Colombia and the Philippines had accessed customer accounts in order to obtain unlock codes for AT&T mobile phones. In Bogota, until May 27, 2014, full Social Security numbers were accessible in the ordinary course of business to three of the managers whose login credentials were used in these activities. After May 27, 2014, AT&T implemented measures to mask full Social Security numbers for AT&T Mobility Call Center managers. AT&T has found no evidence that these or any other managers in Colombia or the Philippines acquired or used the full Social Security numbers of any Affected Customers. In some cases, certain CPNI relating to bill amounts and rate plans were visible at the time of the unauthorized activity, but AT&T's investigation also found no evidence that this information was used. The unauthorized access ceased in the Bogota, Colombia facility in July 2014. In December 2014, AT&T changed its unlock policy and ceased requiring information from customer records before providing an unlock code. This change eliminated the incentive for Covered Employees or Covered Vendor Employees to engage in the activities described above. AT&T informed the Bureau that based on its investigation to date, it had identified approximately 211,000 customer accounts that were accessed in connection with the unlock code activities in the Colombian and Philippines facilities, but that its ongoing investigation could reveal additional instances of such activities. AT&T informed the Bureau that it is in the process of developing new monitoring procedures to identify suspicious account access by call center representatives.

12. The Parties negotiated the following terms and conditions of settlement and hereby enter into this Consent Decree as provided below.

III. TERMS OF AGREEMENT

13. **Adopting Order**. The provisions of this Consent Decree shall be incorporated by the Bureau in an Adopting Order.

14. **Jurisdiction**. AT&T agrees that the Bureau has jurisdiction over it and the matters contained in this Consent Decree and has the authority to enter into and adopt this Consent Decree.

15. **Effective Date; Violations**. The Parties agree that this Consent Decree shall become effective on the Effective Date as defined herein. As of the Effective Date, the Parties agree that this Consent Decree shall have the same force and effect as any other order of the Commission.

16. **Termination of Investigation**. In express reliance on the covenants and representations in this Consent Decree and to avoid further expenditure of public resources, the Bureau agrees to terminate the Investigation and its investigation into matters described in paragraph 11. In consideration for the termination of the Investigation, AT&T agrees to the terms, conditions, and procedures contained herein. The Bureau further agrees that, in the absence of new material evidence relating to the Investigation, it will not use the facts developed in the Investigation through the Effective Date, or the existence of this Consent Decree, to institute any new proceeding, formal or informal, or take any action against AT&T concerning the matters that were the subject of the Investigation, including the matters described in paragraphs 7 through 10, and its investigation into matters described in paragraph 11. The Bureau also agrees that, in the absence of new material evidence relating to the Investigation described in paragraphs 7–10, the investigation into matters described in paragraph 11 and in the absence of any misrepresentation in paragraph 19(a), it will not use the facts developed in the Investigation or its investigation into matters described in paragraph 11 through the Effective Date, or the existence of this Consent Decree, to institute any proceeding, formal or informal, or take any action against AT&T with respect to basic qualifications, including its character qualifications, to be a Commission licensee or hold Commission licenses or authorizations. For purposes of this paragraph, additional instances of unauthorized access to a customer's account in Colombia or the Philippines for the apparent purpose of obtaining an unlock code do not constitute new material evidence. For the purpose of this Consent Decree only, AT&T does not contest that its actions that were the subject of the Investigation violated Section 222(c) of the Act, and Sections 64.2010(a) and 64.2011(b) of the Commission's Rules. It is the intent of the Parties that this Consent Decree shall not be used as evidence or precedent in any action or

proceeding, except in an action to enforce the Consent Decree.

17. **Compliance Officer**. Within thirty (30) calendar days after the Effective Date, AT&T shall designate a senior corporate manager with the requisite corporate and organizational authority to serve as a Compliance Officer and to discharge the duties set forth below. The person designated as the Compliance Officer shall be responsible for developing, implementing, and administering the Compliance Plan and ensuring that AT&T complies with the terms and conditions of the Compliance Plan and this Consent Decree. In addition to the general knowledge of the Communications Laws necessary to discharge his or her duties under this Consent Decree, the Compliance Officer shall have specific knowledge of the information security principles and practices necessary to implement the information security requirements of this Consent Decree, and the specific requirements of Section 222 of the Act, and the CPNI Rules, before assuming his/her duties. The Compliance Officer or managers reporting to the Compliance Officer with responsibilities related to this Consent Decree shall be privacy certified by an industry certifying organization and keep current through appropriate continuing privacy education courses.

18. **Compliance Plan**. For purposes of settling the matters set forth herein, AT&T agrees that it shall, within ninety (90) calendar days after the Effective Date, develop and implement a Compliance Plan designed to ensure future compliance with the Communications Laws and with the terms and conditions of this Consent Decree. AT&T will implement, at a minimum, the following procedures:

(a) **Risk Assessment**. Within ninety (90) calendar days after the Effective Date, AT&T shall complete a risk assessment reasonably designed to identify internal risks of unauthorized access, use, or disclosure of Personal Information and CPNI by Covered Employees and Covered Vendor Employees (Risk Assessment). The Risk Assessment must evaluate the sufficiency of existing policies, procedures, and other safeguards in place to control the risk of such unauthorized access, use, or disclosures.

(b) **Information Security Program**. Within ninety (90) calendar days after the Effective Date, AT&T shall have in place and thereafter maintain an information security program reasonably designed to protect CPNI and Personal Information from unauthorized access, use, or disclosure by Covered Employees and Covered Vendor Employees (Information Security Program). AT&T shall ensure that the Information Security Program is fully documented in writing (including, as appropriate, within the Operating Procedures/Compliance Manual described below) and includes: (i) administrative, technical, and physical safeguards reasonably designed to protect the security and confidentiality of Personal Information and CPNI; (ii) reasonable measures to protect Personal Information and CPNI maintained by or made available to Vendors, Covered Employees, and Covered Vendor Employees, including exercising due diligence in selecting Vendors, requiring Vendors by contract to implement and maintain administrative, technical, and physical safeguards for the protection of Personal Information and CPNI, and engaging in ongoing monitoring of Vendors' compliance with their security obligations and implementing measures to sanction Vendors that fail to comply with their security obligations (including, where appropriate, terminating AT&T's relationship with such Vendors); (iii) access controls reasonably designed to limit access to Personal Information and CPNI to authorized AT&T employees, agents, and Covered Vendor Employees; (iv) reasonable processes to assist AT&T in detecting and responding to suspicious or anomalous account activity, including whether by malware or otherwise, involving Covered Employees and Covered Vendor Employees: (v) a comprehensive breach response plan that will enable AT&T to fulfill its obligations under applicable laws, with regard to breach

notifications, including its obligations under paragraph 20 while that paragraph remains in effect.

(c) **Ongoing Monitoring and Improvement.** AT&T shall monitor its Information Security Program on an ongoing basis to ensure that it is operating in a manner reasonably calculated to control the risks identified through the Risk Assessment, to identify and respond to emerging risks or threats, and to comply with the requirements of Section 222 of the Act, the CPNI Rules, and this Consent Decree. To the extent that such monitoring reveals that the program is deficient or no longer reasonably fulfills this purpose, AT&T shall implement additional safeguards to address these deficiencies and gaps. Such additional safeguards shall be implemented within a reasonable period of time, taking into account the seriousness of the deficiencies or gaps and the steps necessary to address them.

(d) **Compliance Review.** Within ninety (90) calendar days after the Effective Date, AT&T shall commence a formal internal review of its Information Security Program using procedures and standards generally accepted in the information privacy field. This formal internal review shall be directed by AT&T's Corporate Compliance Unit by professionals with the requisite privacy certifications necessary to review and assess information security programs. Such assessment shall be completed within one hundred and fifty (150) calendar days after the Effective Date, and AT&T shall submit a copy of the written assessment findings to the Commission within ten (10) calendar days of the assessment's completion.

(e) **Compliance Manual**. Within one hundred and twenty (120) calendar days after the Effective Date, the Compliance Officer shall develop and distribute a Compliance Manual to all Covered Employees and to all Vendors with instructions to Vendors to distribute a copy of the Compliance Manual to all Covered Vendor Employees within thirty (30) days and to certify that such distribution has been completed. If such certification is not provided, AT&T will pursue any remedy available to require distribution and certification, including, if necessary, termination of the relationship. Additionally, AT&T shall instruct all Vendors to deliver a Compliance Manual to all future Covered Vendor Employees within thirty (30) calendar days after such future Covered Vendor Employee assumes such position or responsibilities.

(f) The Compliance Manual shall explain the requirements of Sections 222 of the Act, the CPNI Rules, and this Consent Decree, and set forth the Operating Procedures that Covered Employees and Covered Vendor Employees shall follow to help ensure AT&T's compliance with the Act, Rules, and this Consent Decree. AT&T shall periodically review and revise the Compliance Manual and Operating Procedures as necessary to ensure that the information set forth therein remains current and accurate. AT&T shall distribute any revisions to the Compliance Manual to all Covered Employees and all Vendors within thirty (30) calendar days of making such revisions.

(g) **Compliance Training Program.** AT&T shall establish and implement a Compliance Training Program on compliance with Section 222, the CPNI Rules, and the Operating Procedures. As part of the Compliance Training Program Covered Employees shall be advised of AT&T's reporting obligations under paragraph 20 of this Consent Decree and shall be instructed on how to disclose noncompliance with Section 222, the CPNI Rules and the Operating Procedures to the Compliance Officer or his designees. All Covered Employees shall be trained pursuant to the Compliance Training program within six (6) months after the Effective Date, and, any person who becomes a Covered Employee at any time after the initial Compliance Training Program shall be trained within thirty (30) calendar

days after the date such person becomes a Covered Employee. AT&T shall repeat compliance training on an annual basis, and shall periodically review and revise the Compliance Training Program as necessary to ensure that it remains current and complete and to enhance its effectiveness. AT&T shall request, and where permitted by contract require, all Vendors to provide the training to all Covered Vendor Employees within six (6) months after the Effective Date, except that any person who becomes a Covered Vendor Employee at any time after the initial Compliance Training Program shall be trained within thirty (30) calendar days after the date such person becomes a Covered Vendor Employee. AT&T shall request, and where permitted by contract, require Vendors to repeat compliance training on an annual basis.

19. **Terms Specific to Call Centers in Colombia and the Philippines**.

(a) AT&T represents and warrants that it engaged independent third parties to investigate the activities in Bogota, Colombia and to assist with employee interviews in connection with AT&T's investigation of call centers in the Philippines. AT&T further represents and warrants that it has no evidence and no reason to believe that any CPNI or any Personal Information was obtained or used during the course of the activities described in paragraphs 7–11, AT&T further represents and warrants that, effective December 11, 2014, it changed its device unlock policy and no longer requires information contained in AT&T customer records in order to obtain an unlock code, thereby eliminating the incentive for the activities described in paragraphs 7–11. After reasonable diligence, and based on information currently available, including AT&T's change in its unlock policy, AT&T believes that the activities described in paragraph 11 have ceased. AT&T further represents and warrants that it has reported to the Bureau all known instances in which it has reasonably concluded that a Data Breach occurred in Colombia and Philippines call centers. AT&T further represents and warrants that it is continuing to investigate call centers in Colombia and the Philippines for Data Breaches.

(b) Within thirty (30) calendar days of the Effective Date, AT&T shall:

i. Begin a process to provide each Affected Customer written notice that his or her account, including Personal Information and/or CPNI, had been accessed by persons without authorization in violation of AT&T's privacy and security policies and include an offer of one year of complimentary credit monitoring services through a nationally recognized credit monitoring service, such as CSID Protector. The complimentary credit monitoring services offered to each Affected Customer shall include, at a minimum, single bureau credit report and monitoring; court record monitoring and public records searches; non-credit loan searches; identity theft insurance at no cost to Affected Customers; and full service identity theft restoration services. Each written notice provided to Affected Customers shall include the toll-free telephone numbers and web addresses of the major credit reporting agencies. AT&T shall complete such notification within 60 days.

ii. AT&T shall provide a toll-free number where Affected Customers may contact AT&T with questions about the impact of these activities, if any, on their account information.

iii. Subparagraphs 19(b)(i)–(ii) shall also apply to Affected Customers who are identified after the Effective Date and AT&T shall provide the notice required pursuant to subparagraph 19(b) to such customers within thirty (30) calendar days of AT&T's discovery that such customers' accounts were illegally accessed.

20. **Reporting Noncompliance and Data Breaches**. AT&T shall report any noncompliance with the terms and conditions of this Consent Decree within fifteen (15) calendar days after discovery of such noncompliance. Such reports shall include a detailed explanation of: (i) each known instance of noncompliance; (ii) the steps that AT&T has taken or will take to remedy such noncompliance; (iii) the schedule on which such remedial actions will be taken; and (iv) steps that AT&T has taken or will take to prevent the recurrence of any such noncompliance. AT&T shall also report to the FCC any breaches of Personal Information or CPNI involving any Covered Employees or Covered Vendor Employees that AT&T is required by any federal or state law to report to any Federal or state entity or any individual. Reports shall be submitted no later than seven (7) business days after completion of the notification required by federal or state authorities. Such reports shall include (i) the date the breach was reported, (ii) the applicable Federal and state authorities to whom the breach was reported, (iii) copies of the reports AT&T submitted to the applicable state authorities, and (iv) the reference number generated by the central reporting facility for CPNI reports made pursuant to 47 C.F.R. § 64.2011(b). All reports of noncompliance shall be submitted to the Chief, Telecommunications Consumers Division, Enforcement Bureau, Federal Communications Commission, 445 12th Street, SW, Rm. 4C-224, Washington, DC 20554, with copies submitted electronically to David.Valdez@fcc.gov and Michael.Epshteyn@fcc.gov. The foregoing reporting requirement does not affect AT&T's obligations to report data breaches to other regulatory authorities in accordance with applicable law.

21. **Compliance Reports**. AT&T shall file compliance reports with the Commission six (6) months after the Effective Date, twelve (12) months after the Effective Date, twenty-four (24) months after the Effective Date, and thirty-six (36) months after the Effective Date.

(a) Each Compliance Report shall include a detailed description of AT&T's efforts during the relevant period to comply with the terms and conditions of this Consent Decree. In addition, each Compliance Report shall include a certification by the Compliance Officer, as an agent of and on behalf of AT&T, stating that the Compliance Officer has personal knowledge that AT&T: (i) has established and implemented the Compliance Plan; (ii) has utilized the Operating Procedures since the implementation of the Compliance Plan; and (iii) is not aware of any instances of noncompliance with the terms and conditions of this Consent Decree, including the reporting obligations set forth in paragraph 20 of this Consent Decree.

(b) The Compliance Officer's certification shall be accompanied by a statement explaining the basis for such certification and shall comply with Section 1.16 of the Rules and be subscribed to as true under penalty of perjury in substantially the form set forth therein.[36]

(c) If the Compliance Officer cannot provide the requisite certification, the Compliance Officer, as an agent of and on behalf of AT&T, shall provide the Commission with a detailed explanation of the reason(s) why and describe fully: (i) each instance of noncompliance; (ii) the steps that AT&T has taken or will take to remedy such noncompliance, including the schedule on which proposed remedial actions will be taken; and (iii) the steps that AT&T has taken or will take to prevent the recurrence of any such noncompliance, including the schedule on which such preventive action will be taken.

[36] *See* 47 C.F.R. § 1.16.

(d) All Compliance Reports shall be submitted to the Chief, Telecommunications Consumers Division, Enforcement Bureau, Federal Communications Commission, 445 12th Street, SW, Rm. 4C-224, Washington, DC 20554, with a copy submitted electronically to David.Valdez@fcc.gov and Michael.Epshteyn@fcc.gov.

22. **Termination Date**. With the exception of paragraphs 18(b)–(c), the requirements set forth in paragraphs 17 through 21 of this Consent Decree shall expire thirty-six (36) months after the Effective Date. The requirements set forth in paragraphs 18(b)–(c) shall expire seven (7) years after the Effective Date.

23. **Section 208 Complaints; Subsequent Investigations**. Nothing in this Consent Decree shall prevent the Commission or its delegated authority from adjudicating complaints filed pursuant to Section 208 of the Act[37] against AT&T or its affiliates for alleged violations of the Act, or for any other type of alleged misconduct, regardless of when such misconduct took place. The Commission's adjudication of any such complaint will be based solely on the record developed in that proceeding. Except as expressly provided in this Consent Decree, this Consent Decree shall not prevent the Commission from investigating new evidence of noncompliance by AT&T with the Communications Laws.

24. **Civil Penalty**. AT&T will pay a civil penalty to the United States Treasury in the amount of $ 25 million ($25,000,000) within thirty (30) calendar days after the Effective Date. AT&T shall send electronic notification of payment to Johnny Drake, Telecommunications Consumers Division, Enforcement Bureau, Federal Communications Commission at Johnny.Drake@fcc.gov on the date said payment is made. The payment must be made by check or similar instrument, wire transfer, or credit card, and must include the Account Number and FRN referenced above. Regardless of the form of payment, a completed FCC Form 159 (Remittance Advice) must be submitted.[38] When completing the FCC Form 159, enter the Account Number in block number 23A (call sign/other ID) and enter the letters "FORF" in block number 24A (payment type code). Below are additional instructions that should be followed based on the form of payment selected:

- Payment by check or money order must be made payable to the order of the Federal Communications Commission. Such payments (along with the completed Form 159) must be mailed to Federal Communications Commission, P.O. Box 979088, St. Louis, MO 63197-9000, or sent via overnight mail to U.S. Bank – Government Lockbox #979088, SL-MO-C2-GL, 1005 Convention Plaza, St. Louis, MO 63101.
- Payment by wire transfer must be made to ABA Number 021030004, receiving bank TREAS/NYC, and Account Number 27000001. To complete the wire transfer and ensure appropriate crediting of the wired funds, a completed Form 159 must be faxed to U.S. Bank at (314) 418-4232 on the same business day the wire transfer is initiated.
- Payment by credit card must be made by providing the required credit card information on FCC Form 159 and signing and dating the Form 159 to authorize the credit card payment. The completed Form 159 must then be mailed to Federal Communications Commission, P.O. Box 979088, St. Louis, MO 63197-9000, or sent via overnight mail to U.S. Bank – Government Lockbox #979088, SL-MO-C2-GL, 1005 Convention Plaza, St. Louis, MO 63101.

Questions regarding payment procedures should be addressed to the Financial Operations Group Help Desk by phone, 1-877-480-3201, or by e-mail, ARINQUIRIES@fcc.gov.

[37] 47 U.S.C. § 208.

[38] An FCC Form 159 and detailed instructions for completing the form may be obtained at http://www.fcc.gov/Forms/Form159/159.pdf.

25. **Waivers**. As of the Effective Date, AT&T waives any and all rights it may have to seek administrative or judicial reconsideration, review, appeal or stay, or to otherwise challenge or contest the validity of this Consent Decree and the Adopting Order. AT&T shall retain the right to challenge Commission interpretation of the Consent Decree or any terms contained herein. If either Party (or the United States on behalf of the Commission) brings a judicial action to enforce the terms of the Consent Decree or the Adopting Order, neither AT&T nor the Commission shall contest the validity of the Consent Decree or the Adopting Order, and AT&T shall waive any statutory right to a trial *de novo*. AT&T hereby agrees to waive any claims it may otherwise have under the Equal Access to Justice Act[39] relating to the matters addressed in this Consent Decree.

26. **Severability**. The Parties agree that if any of the provisions of the Consent Decree shall be held unenforceable by any court of competent jurisdiction, such unenforceability shall not render unenforceable the entire Consent Decree, but rather the entire Consent Decree shall be construed as if not containing the particular unenforceable provision or provisions, and the rights and obligations of the Parties shall be construed and enforced accordingly.

27. **Invalidity**. In the event that this Consent Decree in its entirety is rendered invalid by any court of competent jurisdiction, it shall become null and void and may not be used in any manner in any legal proceeding.

28. **Subsequent Rule or Order**. The Parties agree that if any provision of the Consent Decree conflicts with any subsequent Rule or Order adopted by the Commission (except an Order specifically intended to revise the terms of this Consent Decree to which AT&T does not expressly consent) that provision will be superseded by such Rule or Order.

29. **Successors and Assigns**. AT&T agrees that the provisions of this Consent Decree shall be binding on its successors, assigns, and transferees.

30. **Final Settlement**. The Parties agree and acknowledge that this Consent Decree shall constitute a final settlement between the Parties with respect to the Investigation.

31. **Modifications**. Except as provided in paragraph 27, this Consent Decree cannot be modified without the advance written consent of both Parties.

32. **Paragraph Headings**. The headings of the paragraphs in this Consent Decree are inserted for convenience only and are not intended to affect the meaning or interpretation of this Consent Decree.

33. **Authorized Representative**. Each Party represents and warrants to the other that it has full power and authority to enter into this Consent Decree. Each person signing this Consent Decree on behalf of a Party hereby represents that he or she is fully authorized by the Party to execute this Consent Decree and to bind the Party to its terms and conditions.

[39] *See* 5 U.S.C. § 504; 47 C.F.R. §§ 1.1501–1.1530.

34. **Counterparts**. This Consent Decree may be signed in counterpart (including electronically or by facsimile). Each counterpart, when executed and delivered, shall be an original, and all of the counterparts together shall constitute one and the same fully executed instrument.

_____
Travis LeBlanc, Chief
Enforcement Bureau

_____
Date

For: AT&T Services, Inc.

_____
Debbie Storey
Executive Vice President – Mobility Customer Service
AT&T Services, Inc.

_____
Date