Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of	)	
	)	
AT&T Services Inc.	)	File No.: EB-TCD-23-00034851
	)	CD Acct. No.: 202432170008
	)	FRN: 0005193701
	)	
	)	

ORDER

Adopted: September 16, 2024 **Released: September 17, 2024**

By the Chief, Enforcement Bureau:

1. The Enforcement Bureau (Bureau) of the Federal Communications Commission (FCC or Commission) has entered into a Consent Decree to resolve its investigation into whether AT&T Services Inc. (AT&T or Company): (i) failed to meet its duty to protect the confidentiality of customer proprietary information (PI); (ii) improperly used, disclosed, or permitted access to individually identifiable customer proprietary network information (CPNI) without customer approval; (iii) failed to take reasonable measures to discover and protect against attempts to gain access to CPNI; and (iv) engaged in unjust and unreasonable privacy, cybersecurity, and vendor management practices in connection with a data breach of its vendor's cloud environment that occurred in January 2023 (the 2023 Breach). The 2023 Breach occurred when threat actors accessed the vendor's cloud environment and ultimately exfiltrated AT&T customer information that the Company had previously shared with the vendor. The vendor should have destroyed or returned that customer information years prior to the 2023 Breach pursuant to relevant contracts AT&T entered into with the vendor. AT&T failed to ensure its vendor adequately protected that customer information; instead, it remained in the vendor's cloud environment for many years after it should have been deleted or returned to AT&T and was ultimately exposed in the 2023 Breach.

2. In 2023, over 80 percent of data breaches involved data stored in the cloud.[1] Security researchers also singled out the telecommunications sector as the top industry target for cloud attackers in 2023.[2] Cloud misconfigurations and vendor systems were two of the three primary causes of data breaches of personal data in 2023.[3] Data stored in the cloud may become "an easy target" when companies "unintentionally misuse the cloud, such as allowing excessively permissive cloud access, having unrestricted ports, and use unsecured backups."[4] For years, the U.S. government has warned the public that "misconfiguration of cloud resources remains the most prevalent cloud vulnerability" that could be "exploited to access cloud data and services."[5] The growing privacy and cybersecurity risks

[1] Stuart Madnick, *Why Data Breaches Spiked in 2023,* Harvard Business Review (Feb. 19, 2024), https://hbr.org/2024/02/why-data-breaches-spiked-in-2023.

[2] Sysdig, *2023 Global Cloud Threat Report* at 7 (Aug. 2, 2023), https://sysdig.com/content/c/pf-2023-global-cloud-threat-report?x=u_WFRi.

[3] *See supra* note 1.

[4] *Id*.

[5] Nat'l Sec. Agency, *Mitigating Cloud Vulnerabilities* (Jan. 22, 2020), https://media.defense.gov/2020/Jan/22/2002237484/-1/-1/0/CSI-MITIGATING-CLOUD-VULNERABILITIES_20200121.PDF.

associated with cloud security and vendor security make the terms of this Consent Decree even more timely and necessary.

3. The Communications Act of 1934, as amended (Communications Act or Act),[6] and the Commission's rules require that carriers protect consumers' personal information from unauthorized access, use, or disclosure.[7] The Act further imposes vicarious liability on carriers for the acts, omissions, or failures of their agents acting within the scope of their employment.[8] Carriers are responsible for the acts of their agents and contractors.[9] The Commission expects carriers to meet the requirements of the Act and the Commission's rules,[10] including to take "every reasonable precaution" to protect customers' proprietary or personal information.[11] That includes reasonable practices as they relate to cloud security, data retention and disposal, and vendor oversight.

4. The failure to protect the confidentiality of customers' PI violates a carrier's statutory duty under the Act[12] to protect that information. Moreover, impermissibly using, disclosing, or permitting access to individually identifiable CPNI without customer approval, and failing to take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI, violates a carrier's statutory duty under the Act and the requirements of the Commission's CPNI rules, respectively.[13] These failures also constitute an unjust and unreasonable practice in violation of the Act.[14]

5. To settle these matters, AT&T will pay a civil penalty of $13,000,000 and commit to robust terms of agreement to strengthen the Company's data governance practices to ensure appropriate processes and procedures are incorporated into AT&T's business practices to protect consumers' sensitive data against similar vendor data breaches in the future. Specifically, AT&T will be required to improve its privacy and data security practices by, among other things:

(i) **Broad Customer Information Protections:** protecting CPNI and other sensitive personal information pursuant to various terms in the Consent Decree with AT&T agreeing to limit vendor access to and disposal of such information;

(ii) **Comprehensive Information Security Program:** requiring an Information Security Program that is designed to protect the security, confidentiality, and integrity of AT&T customers' information, including CPNI and other sensitive personal information;

(iii) **Multifaceted Vendor Controls and Oversight:** engaging in due diligence when selecting vendors, requiring vendors to employ safeguards for customer information,

[6] 47 U.S.C. §§ 201(b), 222(a), 222(c).

[7] *See id.* § 222; 47 CFR § 64.2001 *et seq.*

[8] 47 U.S.C. § 217.

[9] AT&T is well-aware of this responsibility. *See AT&T, Inc.*, Notice for Apparent Liability for Forfeiture and Admonishment, 35 FCC Rcd 1743, 1759-61, paras. 45-49 (Feb. 28, 2020) (explaining that a carrier cannot avoid its statutory obligations by assigning them to a third party), *aff'd*, *AT&T Location Data Forfeiture Order*, 2024 WL 19052277, *18, para. 51 ("[W]e clearly explained that, pursuant to section 217 of the Act, carriers cannot disclaim their obligations to protect customer CPNI by delegating those obligations to third parties.").

[10] *See, e.g.*, 47 U.S.C. §§ 222, 201(b); 47 CFR § 64.2001, *et seq*.

[11] *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information,* Report and Order and Further Notice of Proposed Rulemaking, 22 FCC Rcd 6927, 6959 at para. 64 n.198 (2007) (*2007 CPNI Order*) (citing 47 U.S.C. § 222(a)).

[12] 47 U.S.C. §222(a).

[13] *See id*. § 222(c); 47 CFR § 64.2010(a).

[14] 47 U.S.C. § 201(b).

limiting vendor access to and storage of customer information, and conducting enhanced vendor oversight;

(iv) **Data Inventory Program:** enhancing the Company's data inventory processes to track AT&T customers' data shared with vendors, allowing AT&T to act more swiftly to protect customer data in the future;

(v) **Data Retention and Disposal**: requiring vendors to adhere to retention and disposal obligations related to customer information, to limit the quantity of customer information vulnerable to breach; and

(vi) **Annual Compliance Audits:** conducting annual compliance audits to evaluate AT&T's compliance with the Consent Decree, including the information security and vendor information security requirements listed above.

6. Implementing the terms contained in this Consent Decree will require AT&T to make significant investments in, and prioritize, the safeguarding of customers' information shared with third parties. Given AT&T's size, number of customers, and extensive use of vendors, this will likely require expenditures far greater than the civil penalty herein. The Commission will hold AT&T accountable for making these mandatory changes to its data protection practices, as required to comply with this Consent Decree, the Communications Act, and the Commission's rules going forward. The Commission long ago determined—and was affirmed by the U.S. Court of Appeals for the D.C. Circuit on "common sense" grounds—that the "risk of unauthorized disclosure of customer information increases with the number of entities possessing it."[15] Companies that choose to share their customers' data with vendors must act as responsible stewards and hold their vendors responsible for protecting that data as required by the Communications Act and the Commission's rules.

7. 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 sections 201(b), 222(a) and (c) of the Act,[16] and section 64.2010(a) of the Commission's rules.[17]

8. In the absence of material new evidence relating to this matter, we do not set for hearing the question of AT&T's basic qualifications to hold or obtain any Commission license or authorization.[18]

9. Accordingly, **IT IS ORDERED** that, pursuant to section 4(i) of the Act, 47 U.S.C. § 154(i), and the authority delegated by sections 0.111 and 0.311 of the Commission's rules, 47 U.S.C. §§ 0.111, 0.311, the attached Consent Decree **IS ADOPTED** and its terms incorporated by reference.

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

[15] *NCTA v. FCC*, 555 F.3d 996, 1001-02 (D.C. Cir. 2009) ("[C]ommon sense supports the Commission's determination that the risk of unauthorized disclosure of customer information increases with the number of entities possessing it."), *aff'g 2007 CPNI Order,* 22 FCC Rcd at 6951, para. 46 ("[I]nformation security breaches are on the rise in this country, and it is axiomatic that the more companies that have access to CPNI, the greater the risk of unauthorized disclosure through disclosure by insiders or computer intrusion.").

[16] 47 U.S.C. §§ 201(b), 222(a), (c).

[17] 47 CFR § 64.2010(a).

[18] *See id.* § 1.93(b).

11. **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 Glenis McKoy, AT&T Services Inc., 601 New Jersey Ave NW, Suite 650, Washington, D.C. 20001.

FEDERAL COMMUNICATIONS COMMISSION

Loyaan A. Egal
Chief
Enforcement Bureau

Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of	)	
	)	
AT&T Services Inc.	)	File No.: EB-TCD-23-00034851
	)	CD Acct. No.: 202432170008
	)	FRN: 0005193701
	)	
	)	

CONSENT DECREE

1. The Enforcement Bureau (Bureau) of the Federal Communications Commission (FCC or Commission) and AT&T Services Inc. (AT&T or the Company), by their authorized representatives, hereby enter into this Consent Decree for the purpose of terminating the Bureau's investigation into whether AT&T violated sections 201(b) and 222 of the Communications Act of 1934, as amended (Communications Act or Act),[1] and section 64.2010(a) of the Commission's Rules[2] in connection with a January 2023 data breach of a vendor's cloud environment (January 2023 breach).[3]

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) "AT&T" means AT&T Services, Inc., and its affiliates, subsidiaries, and successors-in-interest.

(c) "Authorized Retailer" means an entity whose responsibilities include performance of services to sell AT&T products and services to end users and that involve the collection, transmission, processing, access to, use, disclosure, storage, or protection of Covered Data, pursuant to a contractual relationship or agreement with AT&T, provided that Authorized Retailer shall not include any wholesale customer or reseller of AT&T products and services.

(d) "Breach" means when a person, without authorization or exceeding authorization, gains access to, uses, or discloses CPNI. A breach shall not include a good-faith acquisition of CPNI by a Vendor, employee, or agent of AT&T where such information is not used improperly or further disclosed.

(e) "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, including but not limited to the CPNI Rules.

(f) "Compliance Plan" means the compliance obligations, program, and procedures described in this Consent Decree at Paragraph 22.a.

(g) "Covered Data" means CPNI and Sensitive Personal Information.

(h) "Covered Employees" means all employees and agents of AT&T whose responsibilities include performance, direct supervision, oversight, or management

[1] 47 U.S.C. §§ 201, 222.

[2] 47 CFR § 64.2010(a).

[3] Material set off by double brackets {[ ]} is confidential and is redacted from the public version of this document.

of the performance of duties involving the collection, transmission, processing, access to, use, disclosure, storage, or protection of Covered Data, or any duties pursuant to the Privacy and Security Requirements. Covered Employees do not include Covered Vendor Employees.

(i) "Covered Vendor Employees" means all employees and agents of any Vendor whose responsibilities include performance of services involving the collection, transmission, processing, access to, use, disclosure, storage, or protection of Covered Data, or any duties pursuant to the Privacy and Security Requirements.

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

(k) "Customer" means a current or former customer of AT&T.

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

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

(n) "Investigation" means the investigation commenced by the Bureau in EB-TCD-23-00034851.

(o) "Privacy and Security Requirements" means the requirements of section 222 of the Act, as well as the CPNI Rules.

(p) "Sensitive Personal Information" or "SPI" shall mean the categories of information identified as Sensitive Personal Information as of August 6, 2024, in the AT&T Privacy Notice at https://about.att.com/privacy/privacy-notice/state-disclosures.html#sensitive-personal-info.

(q) "Vendor" means any Authorized Retailer, or person or entity subject to the contracting processes managed by AT&T's Global Supply Chain organization, whose responsibilities include performance of either services involving the collection, transmission, processing, access to, use, disclosure, storage, or protection of Covered Data, or any duties pursuant to the Privacy and Security Requirements.

II. BACKGROUND

3. *Legal Framework.* The Act and Commission's Rules govern and limit telecommunications carriers' use and disclosure of certain customer data. Through section 222 of the Act, Congress established a framework for governing telecommunications carriers' use and protection of information received or obtained by virtue of providing a telecommunications service. Section 222(a) imposes on telecommunications carriers a general "duty to protect the confidentiality of proprietary information of, and relating to, . . . customers."

4. Section 222(c) establishes specific privacy requirements for "customer proprietary network information" or CPNI. This includes information relating to the "quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier" and that is "made available to the carrier by the customer solely by virtue of the carrier-customer relationship."[4] It also includes "information contained in the bills pertaining to" telephone service "received by a customer of a carrier," except for subscriber list information.[5]

[4] 47 U.S.C. § 222(h)(1)(A).

[5] 47 U.S.C. § 222(h)(1)(B).

5. The Commission has adopted the CPNI Rules that implement the privacy requirements of section 222.[6] Section 64.2010 of the CPNI Rules, which the Commission adopted in its 2007 CPNI Order,[7] articulates safeguards that carriers must implement to protect CPNI.[8] Section 64.2010(a) requires carriers to "take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI."[9] In adopting section 64.2010(a), the Commission declined to adopt prescriptive security practices.[10] Instead, it "allow[ed] carriers to determine what specific measures will best enable them to ensure compliance with the requirement" and "permit[ted] carriers to weigh the benefits and burdens of particular methods" to "allow carriers to improve the security of CPNI in the most efficient manner possible."[11]

6. Additionally, section 201(b) of the Act sets forth the overarching obligation that common carriers' practices be "just and reasonable" and declares unlawful any practice that is unjust or unreasonable.[12]

7. *Factual Background.* 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.[13] AT&T is one of the largest wireless carriers in the United States, with 241.5 million wireless subscribers, earning $122.4 billion in operating revenue in 2023.[14] AT&T provides these wireless services through its wholly-owned subsidiary, AT&T Mobility LLC (AT&T Mobility).[15]

8. In January 2023, an AT&T vendor, {[ ]} (Vendor X), suffered a data breach that exposed information related to 8,931,656 AT&T Mobility customers.[16] AT&T reported the January 2023 breach to the Data Breach Reporting Portal[17] on February 7, 2023,[18] and filed a supplemental submission on May 15, 2023.[19] Based on AT&T's report, the Bureau opened its

[6] 47 CFR §§ 64.2001-64.2011.

[7] *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, Report and Order and Further Notice of Proposed Rulemaking, 22 FCC Rcd 6927, 6945-46, para. 34 (2007) (*2007 CPNI Order*)).

[8] 47 CFR § 64.2010.

[9] 47 CFR § 64.2010(a).

[10] *See 2007 CPNI Order*, 22 FCC Rcd at 6945-46, para. 34.

[11] *Id.*

[12] 47 U.S.C. § 201(b).

[13] *See* AT&T Inc., *SEC Form 8-K* (Jan. 24, 2024), https://investors.att.com/~/media/Files/A/ATT-IR-V2/financial-reports/quarterly-earnings/2023/4q-2023/ATT_4Q_2023_8_K_Earnings_8_01.pdf [https://perma.cc/XAD4-666Y].

[14] *See id*.

[15] *See* AT&T Inc., *2023 Annual Report and SEC Form 10-K* (Feb. 23, 2024), https://investors.att.com/~/media/Files/A/ATT-IR-V2/financial-reports/annual-reports/2023/2023-complete-annual-report.pdf [https://perma.cc/NX4S-ARWD].

[16] *See* Supplemental Response to Initial Letter of Inquiry, from AT&T Services, Inc., to Shana Yates, Deputy Chief, Telecommunications Consumers Division, et al., FCC Enforcement Bureau at 1, Response to Inquiry 2 (on file in EB-TCD-23-00034851) (Supplemental Response to Initial LOI).

[17] Telecommunications carriers are required to report CPNI breaches through the online portal at https://www.cpnireporting.gov. *See* 47 CFR § 64.2011(b). The data reported through the portal is collected by the U.S. Secret Service and the Federal Bureau of Investigation.

[18] FBI/USSS CPNI Data Breach Reporting Portal Report 2023-775 (Feb. 7, 2023).

[19] FBI/USSS CPNI Data Breach Reporting Portal Report 2023-3326 (May 15, 2023).

investigation into the incident, issuing letters of inquiry[20] to AT&T and subpoenas[21] to Vendor X, and meeting with representatives from both companies. AT&T and Vendor X responded to these inquiries.[22]

9. *AT&T-Vendor X Relationship*. AT&T utilized Vendor X to generate and host personalized video content for AT&T customers, including billing and marketing videos.[23] AT&T shared certain customer information with Vendor X as part of the relationship and in order to receive Vendor X's services.[24] Such information included some elements of CPNI, as well as other customer information.[25]

10. The operative agreements[26] governing the business relationship between AT&T and Vendor X outlined the services that Vendor X would provide to AT&T and articulated Vendor X's

[20] *See, e.g.*, Letter of Inquiry from Kristi Thompson, Chief, Telecommunications Consumers Division, FCC Enforcement Bureau, to AT&T Services, Inc. (Feb. 17, 2023) (on file in EB-TCD-23-00034851); Letter of Inquiry from Kristi Thompson, Chief, Telecommunications Consumers Division, FCC Enforcement Bureau, to AT&T Services, Inc. (Oct. 6, 2023) (on file in EB-TCD-23-00034851); Letter of Inquiry from Kristi Thompson, Chief, Telecommunications Consumers Division, FCC Enforcement Bureau, to AT&T Services, Inc. (May 30, 2023) (on file in EB-TCD-23-00034851).

[21] *See, e.g.*, Subpoena from Kristi Thompson, Chief, Telecommunications Consumers Division, FCC Enforcement Bureau, to Vendor X (Apr. 25, 2023) (on file in EB-TCD-23-00034851); Subpoena from Kristi Thompson, Chief, Telecommunications Consumers Division, FCC Enforcement Bureau, to Vendor X (Nov. 8, 2023) (on file in EB-TCD-23-00034851); *see also* Letter from Kristi Thompson, Chief, Telecommunications Consumers Division, FCC Enforcement Bureau, to Vendor X (Feb. 9, 2024) (2024 Letter) (on file in EB-TCD-23-00034851).

[22] *See, e.g.,* Response to Letter of Inquiry, from AT&T Services, Inc., to Shana Yates, Deputy Chief, Telecommunications Consumers Division, et al., FCC Enforcement Bureau (May 10, 2023) (on file in EB-TCD-23-00034851); Supplemental Response to Initial Letter of Inquiry, from AT&T Services, Inc., to Shana Yates, Deputy Chief, Telecommunications Consumers Division, et al., FCC Enforcement Bureau (on file in EB-TCD-23-00034851); Response to Supplemental Letter of Inquiry, from AT&T Services, Inc., to Shana Yates, Deputy Chief, Telecommunications Consumers Division, et al., FCC Enforcement Bureau (Dec. 5, 2023) (on file in EB-TCD-23-00034851); Response to Supplemental Letter of Inquiry, from AT&T Services, Inc., to Shana Yates, Deputy Chief, Telecommunications Consumers Division, et al., FCC Enforcement Bureau (Jun. 28 2024) (on file in EB-TCD-23-00034851); Response to Subpoena, from Vendor X, to Shana Yates, Deputy Chief, Telecommunications Consumers Division, et al., FCC Enforcement Bureau (Jun. 23, 2023) (on file in EB-TCD-23-00034851); Response to Supplemental Subpoena, from Vendor X, to Shana Yates, Deputy Chief, Telecommunications Consumers Division, et al., FCC Enforcement Bureau (Dec. 14, 2023) (on file in EB-TCD-23-00034851); Response to Supplemental Subpoena, from Vendor X, to Shana Yates, Deputy Chief, Telecommunications Consumers Division, et al., FCC Enforcement Bureau (Dec. 21 2023) (on file in EB-TCD-23-00034851); Response to 2024 Letter, from Vendor X to Shana Yates, Deputy Chief, Telecommunications Consumers Division, et al., FCC Enforcement Bureau (Feb. 16 2024) (on file in EB-TCD-23-00034851).

[23] *See* Initial LOI Response at 5, Response to Inquiry 5(a). In addition, Vendor X provided device upgrade videos, bill summary and explanation videos, "Welcome to Uverse" videos for new customers of AT&T Uverse products, and new wireless device onboarding services. *Id*.

[24] *See* Initial LOI Response at 5, Response to Inquiry 5(a).

[25] *See id*. at 5, Response to Inquiry 4(k)-4(l); Response to Supplemental Letter of Inquiry, from AT&T Services, Inc., to Shana Yates, Deputy Chief, Telecommunications Consumers Division, et al., FCC Enforcement Bureau at 9, Response to Inquiries 10(a) and 10(d) (Dec. 5, 2023) (on file in EB-TCD-23-00034851) (Supplemental LOI Response). More specifically, the billing information implicated by the January 2023 breach includes: past due balances, balance due, payments, monthly recurring charges, usage information, foundation account numbers; the plan type information includes plan type, name, and features. *See* Initial LOI Supplemental Response at 1, Response to Inquiry 4(f).

[26] The agreements that governed the customer information exposed in the January 2023 breach included {[ ]} between AT&T and Vendor X, as well as {[ ]} between AT&T and {[ ]} (Supplier 1), to which Vendor X subcontracted. Supplier 1 was required to bind all subcontractors, including Vendor X, to the terms of its master agreements with AT&T. *See* Initial LOI Response at 6, Response to Inquiry 5(c).

obligations as they related to AT&T's customers' information. AT&T required Vendor X to meet specific requirements with regard to use, protection, and eventual return or disposal of AT&T customer information. In particular, the relevant agreements required that AT&T's customer data be deleted, destroyed, or returned—either upon expiration or termination of the agreement[27] or when the data was no longer necessary to fulfill contractual obligations.[28]

11. Vendor X was also subject to AT&T's Supplier Information Security Requirements (SISR),[29] which included encryption requirements, access control requirements, and network oversight requirements.[30] Through the SISR, AT&T could assess Vendor X's security practices, including through supplier self-attestation reviews and technical assessments.[31] AT&T stated that, through its supplier monitoring processes, AT&T specifically asks suppliers whether all AT&T records in their possession have been or will be destroyed in accordance with applicable contracts.[32]

12. AT&T shared certain customer CPNI and other customer information with Vendor X, including the customer information exposed in the January 2023 breach.[33] According to AT&T, regardless of which operative agreement governed, the customer information exposed in the January 2023 breach should have been securely destroyed or deleted in 2017 or 2018.[34] AT&T performed multiple reviews and assessments of Vendor X and Supplier 1 between 2016 and 2020.[35] In response to such inquiries, Vendor X and Supplier 1 both stated that they were destroying data in accordance with their respective agreements.[36]

13. *January 2023 breach*. Between January 1 and January 8, 2023, threat actors gained unauthorized access to AT&T customer information.[37] The threat actor accessed and exfiltrated AT&T's

[27] ATT_SS_LOI_00000480, {[ ]} the underlying terms regarding protection, disclosure, and return/destruction of customer information remained in place. *See* ATT_SS_LOI_00000517, Agreement No. 20110824.054.A.001 (2015); ATT_SS_LOI_00000470, Agreement No. 20110824.054.A.002 (2015); ATT_SS_LOI_00000477, Agreement No. 2011824.054.A.003 (2016), ATT_SS_LOI_00000473, Agreement No. 11497.A.003 (2017) (collectively, {[ ]}.

[28] Initial LOI Response at 6, Response to Inquiry 5(c) ("Accordingly, . . . [Vendor X] and/or [Supplier 1] were legally required to securely destroy or return each of the data sets accessed in the [Vendor X] Incident"). *See also,* ATT_SS_LOI_00000069 at 00000125, Software and Professional Services Agreement No. 54258.C, Section 3.38, "Ownership of AT&T Data and AT&T Derived Data"; ATT_SS_LOI_00000256 at 00000320-321, AT&T Agreement No. 53258.A.005, Section 3.38, "Ownership of AT&T Data and AT&T Derived Data".

[29] *See* Initial LOI Response at 19-20, Response to Inquiry 29(c).

[30] AT&T's SISR is a continually updated set of requirements that govern the treatment of customer information by AT&T's suppliers and vendors. The SISR required encryption of a range of confidential or proprietary data and information, and these encryption requirements did not change in updates made to the SISR during the contract period. *See* Supplemental LOI Response at 6, Response to Inquiry 4; *see also* ATT-SS-LOI-00000193 at 00000198, Amendment 2 to Agreement No. 53258.C; ATT_SS_LOI_00000517 at 00000518, {[ ]}.

[31] *See* Initial LOI Response at 19, Response to Inquiry 29(c).

[32] Supplemental LOI Response at 3-4, Response to Inquiry 2(a).

[33] *See* Initial LOI Response at 6, Response to Inquiry 5(c).

[34] *See id*.

[35] Supplemental LOI Response at 3-4, Response to Inquiry 2(a).

[36] *Id.*; *see also*, *e.g.*, ATT_SS_LOI_00005799 (Rows 19, 20), ATT_SS_LOI_00005800 (Rows 45, 46), ATT_SS_LOI_00005801 (Rows 26, 64, and 65).

[37] *See* Initial LOI Response at 2-3, Response to Inquiry 1; ATT_SS_SLOI_00002780, {[ ]} (Forensic Report).

customers' data.[38] AT&T notified Vendor X of the suspected attack on Vendor X's systems on January 6, 2023.[39] The underlying vulnerability was fixed on January 6, 2023, and the forensic investigation did not identify any additional unauthorized activity after January 8, 2023.[40]

14. According to AT&T, the exposed data was shared with Vendor X during the period of 2015 to 2017.[41] The affected data included discrete elements of CPNI (line count for all impacted customers, and bill balance and payment information and rate plan name and features for approximately one percent of impacted customers) and other customer information.[42] While not every customer had each type of data exposed, the January 2023 breach involved 8,931,656 AT&T Mobility customers.[43] AT&T stated that it monitored impacted customer accounts following the incident and identified no evidence of AT&T account-related fraud or other unlawful or unauthorized activity tied to the Breach.[44] According to AT&T, porting, SIM swap, and equipment fraud rates for impacted customers following the incident were consistently less than the rates for the general population of AT&T Mobility customers across all account types.[45]

15. To resolve this matter, the Parties negotiated the following terms and conditions of settlement and enter into this Consent Decree as provided below.

III. TERMS OF AGREEMENT

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

17. **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.

18. **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.

19. **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. 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, 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 on its own motion against AT&T concerning the matters that were the subject of the investigation or to set for hearing the question of AT&T basic qualifications to be a Commission licensee or hold Commission licenses or authorizations based on the matters that were the subject of the investigation.[46]

20. **Admission**. AT&T admits for the purpose of this Consent Decree and for Commission civil enforcement purposes, and in express reliance on the provisions of paragraph 19 herein, that

[38] *See* Initial LOI Response at 2-3, Response to Inquiry 1; ATT_SS_SLOI_00002780, Forensic Report at 4-5.

[39] *See* Initial LOI Response at 2, Response to Inquiry 1.

[40] *See* ATT_SS_SLOI_00002780, Forensic Report at 4-5.

[41] *See* Initial LOI Response at 5, Response to Inquiry 5(b).

[42] *See id.* at 2, Response to Inquiry 1.

[43] *See* Supplemental Response to Initial LOI at 1, Response to Inquiry 2.

[44] *See* Initial LOI Response at 7-8, Response to Inquiry 7; *see also id.* at 12, Response to Inquiry 14.

[45] *Id.* at 7-8, Response to Inquiry 7.

[46] *See* 47 CFR § 1.93(b).

paragraphs 7-14 contain a true and accurate description of the facts underlying the Investigation. No other admissions are made by AT&T.

21. **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.

(a) In addition to the general knowledge of the Privacy and Security Requirements 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 requirements of this Consent Decree, and the Privacy and Security Requirements, 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 or otherwise demonstrate they have equivalent privacy experience through relevant experience.

22. **Compliance Plan and Manual**.

(a) *Compliance Plan*

i. AT&T must, within ninety (90) calendar days after the Effective Date, develop and implement a Compliance Plan designed to ensure compliance with the terms and conditions of this Consent Decree and the CPNI Rules related to such compliance.

(b) *Compliance Manual*

i. The Compliance Officer shall, within one-hundred and twenty (120) calendar days after the Effective Date, develop and maintain a Compliance Manual.

ii. The Compliance Manual shall explain the terms and conditions of this Consent Decree and the CPNI Rules related to such compliance. The Compliance Plan shall set processes and procedures that Covered Employees and Vendors shall follow to ensure AT&T's compliance.

iii. AT&T shall review the Compliance Manual periodically and revise it as necessary to ensure that the information set forth therein remains current and accurate.

(c) *Compliance Manual Distribution*

i. The Compliance Officer shall, within one-hundred and twenty (120) calendar days after the Effective Date, distribute the Compliance Manual to all Covered Employees.

ii. For any future Covered Employees, the Compliance Officer shall distribute the Compliance Manual within thirty (30) calendar days after such future Covered Employee assumes their position or responsibilities.

iii. The Compliance Officer shall, within one-hundred and twenty (120) calendar days after the Effective Date, distribute to all Vendors the Compliance Manual with instructions to Vendors to distribute a copy of the Compliance Manual to all Covered Vendor Employees within thirty (30)

calendar days, and to certify that such distribution has been completed. If such certification is not provided, AT&T will timely pursue appropriate remedies available, including contractual remedies and, if necessary, termination of the relationship, consistent with the sensitivity of the Covered Data processed by the Vendor as well as the nature of the relationship between the Vendor and AT&T to require distribution and certification.

iv. 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.

v. 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.

(d) *Compliance Training Program*

i. AT&T shall establish and implement, or revise as necessary to comply with this Consent Decree, a Compliance Training Program regarding compliance with the Privacy and Security Requirements and the requirements of this Consent Decree. As part of the Compliance Training Program, Covered Employees shall be advised of AT&T's reporting obligations under Paragraph 28 of this Consent Decree and shall be instructed on how to disclose noncompliance with the Consent Decree to the Compliance Officer or his/her designees.

ii. 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.

iii. 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.

23. **Information Security Program**. Within ninety (90) calendar days after the Effective Date, AT&T shall implement, or revise as necessary to comply with this Consent Decree, and thereafter maintain and document, a comprehensive Information Security Program that is reasonably designed to protect the security, confidentiality, and integrity of Covered Data from unauthorized access, use, or disclosure (the Information Security Program). AT&T's Information Security Program must be consistent with principles identified by applicable laws and must consider relevant standards, including, but not limited to, the National Institute of Standards and Technology (NIST) Cybersecurity Framework. At least once every six (6) months, AT&T must review and update the Information Security Program as reasonably necessary. At a minimum, AT&T's Information Security Program must address the following:

(a) Administrative, technical, and physical safeguards, from internal and external risks, that:

i. are based on the volume and sensitivity of the Covered Data at risk; and

ii. are reasonably designed to protect the security, confidentiality, and integrity of Covered Data.

(b) The following reasonable measures to protect Covered Data maintained by or made available to Covered Employees, Vendors, and Covered Vendor Employees:

i. the exercise of due diligence in selecting Vendors capable of reasonably safeguarding Covered Data;

ii. requiring Vendors in writing to implement and maintain administrative, technical, and physical safeguards for the protection of Covered Data;

iii. access controls reasonably designed to limit access to Covered Data to authorized Covered Employees, Vendors, and Covered Vendor Employees;

iv. reasonable limitations on the storage and sharing of Covered Data to that which is reasonably necessary to achieve current business requirements;

v. a comprehensive Breach response plan that will enable AT&T to fulfill its Breach notification obligations under applicable laws; and

vi. timely remediation of critical and high-risk security vulnerabilities related to Covered Data.

(c) A Vendor information security program to require a written certification, consistent with the Vendor information security standards, regarding secure destruction or return of Covered Data that is no longer reasonably necessary to achieve current business requirements, and incorporating the Vendor oversight benchmarks; and

(d) A data inventory program consisting of requirements to enhance data inventory processes reasonably designed to track AT&T Covered Data and to make reasonable efforts to populate and maintain data inventories to track AT&T Covered Data created or stored by AT&T, or transferred to a Vendor.

24. **Vendor Oversight**.

(a) AT&T shall engage in ongoing monitoring of Vendors' compliance with AT&T's data security obligations using assessments, reviews, and other oversight. AT&T shall implement, or revise as necessary to comply with this Consent Decree, measures to sanction Vendors that fail to comply with such data security obligations (including, where appropriate and based on information available to AT&T at the time, terminating AT&T's relationship with such parties).

i. Within nine (9) months of the Effective Date, AT&T shall take reasonable steps to require Vendors to identify Covered Data that is no longer reasonably necessary to achieve current business requirements.

ii. Within six (6) months of the Effective Date, AT&T shall establish, or revise as necessary to comply with this Consent Decree, and thereafter maintain, its Vendor information security program, consistent with the requirements of this section. The Vendor information security program shall be documented in the Compliance Manual and include, at a minimum, Vendor information security standards and benchmarks for Vendor oversight.

(b) *Vendor information security standards.* AT&T will establish, or revise as necessary to comply with this Consent Decree, information security standards for Vendors in

the Compliance Manual, consistent with the Information Security Program. Such standards will require, at a minimum:

i. compliance with all Consent Decree requirements applicable to Vendors;

ii. compliance with AT&T Supplier Information Security Requirements ("SISR");

iii. compliance with data retention and disposal requirements; and

iv. certification of compliance with Consent Decree requirements; SISR; and data retention and disposal requirements, with such certification to occur at intervals designated by AT&T but no less than annually.

(c) *Vendor oversight benchmarks*. AT&T will perform assessments, reviews, and other oversight of Vendor compliance with the Vendor information security standards. AT&T will take into account risks posed to the security of Covered Data when determining the level of assessment review or other oversight for each Vendor. AT&T will ensure that assessments and reviews satisfy minimum volume benchmarks, including a minimum of twenty percent (20%) of Vendors each year, inclusive of assessments or reviews of:

i. all new Vendors on or before twelve (12) months of initial contracting date and thirty-six (36) months of initial contracting date, provided that the latter engagement is required only to the extent the Vendor's engagement remains active for a continuous period of more than 36 months;

ii. any Vendor that experiences a Breach, which, unless terminated, shall promptly be subject to an assessment or review following the Breach; and

iii. any Vendor that does not conform with the Vendor information security standards, which, unless terminated, shall be subject to annual assessments or reviews for a period of at least three (3) years.

25. **Data Inventory Program**. AT&T shall take steps to enhance its data inventory processes as part of a Data Inventory Program reasonably designed to track AT&T Covered Data that is: (i) contained in AT&T's networks, systems, and assets; and (ii) transferred or otherwise made available to a Vendor. In connection with such enhancement, AT&T shall document and maintain policies, procedures, standards, and technical measures applicable to data inventories. AT&T shall make reasonable efforts to complete such process enhancements within two (2) years of the Effective Date, after which AT&T will make reasonable efforts to populate and maintain the inventories to track AT&T Covered Data created or stored, or transferred or otherwise made available to a Vendor, on or after such date.

26. **Data Retention and Disposal**.

(a) AT&T must require Vendors to retain Covered Data only as reasonably necessary to accomplish AT&T's current business requirements for sharing such information or as otherwise required by law.

(b) AT&T must require Vendors to adhere to requirements regarding data retention for Covered Data that are consistent with AT&T's internal retention policies and schedules. Such requirements must set forth a set time frame or other criteria for deletion of such Covered Data.

(c) AT&T must obtain a written certification of such deletion, disposal, or return from the relevant Vendor consistent with Paragraph 24.b.iv, above.

27. **Compliance Audits**.

(a) *Compliance Audits*.

i. AT&T shall conduct annual compliance audits to evaluate AT&T's compliance with this Consent Decree (the "Compliance Audits").

ii. Such Compliance Audits shall consider, at a minimum, the compliance of applicable business units with the requirements and operating procedures set forth in the Compliance Manual; the Information Security Program requirements; the requirements set forth in the Vendor Oversight, Data Inventory Program, and Data Retention and Disposal sections of this Consent Decree.

28. **Reporting Noncompliance**. AT&T shall report any material noncompliance with the terms and conditions of this Consent Decree within thirty (30) calendar days 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. All reports of noncompliance shall be submitted to the Chief, Telecommunications Consumers Division, Enforcement Bureau, Federal Communications Commission, 45 L Street, NE, Washington, DC 20554, with copies submitted electronically to Shana.Yates@fcc.gov, Kimbarly.Taylor@fcc.gov, Lauren.Merk@fcc.gov, Samuel.Hanks@fcc.gov and EB-TCD-Privacy@fcc.gov.

29. **Compliance Reports**.

(a) AT&T shall file compliance reports with the Commission six (6) months after the Effective Date, twelve (12) months after the Effective Date, and then annually on the anniversary of the Effective Date for the term of this Consent Decree.

(b) Each Compliance Report shall include:

i. 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 required by Paragraph 22.a of the Consent Decree; (ii) has utilized the Information Security Program since the implementation of the Compliance Plan; and (iii) is not aware of any instances of material noncompliance with the terms and conditions of this Consent Decree, including the reporting obligations set forth in Paragraph 28 of this Consent Decree.

ii. The Compliance Officer's certification described in Paragraph 29.b.i, above, 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.[47]

(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 material 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 AT&T has taken or will take to prevent the

[47] 47 CFR § 1.16.

recurrence of any such noncompliance, including the schedule on which such preventive action will be taken.

(d) All Compliance Reports shall be submitted to the Chief, Telecommunications Consumers Division, Enforcement Bureau, Federal Communications Commission, 45 L Street, NE, Washington, DC 20554, with copies submitted electronically to Shana.Yates@fcc.gov, Kimbarly.Taylor@fcc.gov, Lauren.Merk@fcc.gov, Samuel.Hanks@fcc.gov, and EB-TCD-Privacy@fcc.gov.

30. **Termination Date**. Unless otherwise indicated, the requirements set forth in this Consent Decree shall expire three (3) years after the Effective Date.

31. **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[48] 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.

32. **Civil Penalty**. AT&T will pay a civil penalty to the United States Treasury in the amount of $13,000,000 within thirty (30) calendar days of the Effective Date.

AT&T acknowledges and agrees that upon execution of this Consent Decree, the Civil Penalty shall become a "Claim" or "Debt" as defined in 31 U.S.C. § 3701(b)(1).[49] Upon an Event of Default, all procedures for collection as permitted by law may, at the Commission's discretion, be initiated. AT&T shall send electronic notification of payment to Kimbarly.Taylor@fcc.gov and EB-TCD-Privacy@fcc.gov on the date said payment is made. Payment of the Civil Penalty must be made by credit card using the Commission's Registration System (CORES) at https://apps.fcc.gov/cores/userLogin.do, ACH (Automated Clearing House) debit from a bank account, or by wire transfer from a bank account. The Commission no longer accepts Civil Penalty payments by check or money order. Below are instructions that payors should follow based on the form of payment selected:[50]

- Payment by wire transfer must be made to ABA Number 021030004, receiving bank TREAS/NYC, and Account Number 27000001. In the OBI field, enter the FRN(s) captioned above and the letters "FORF". In addition, a completed Form 159[51] or printed CORES form[52] must be faxed to the Federal Communications Commission at 202-418-2843 or e-mailed to RROGWireFaxes@fcc.gov on the same business day the wire transfer is initiated. Failure to provide all required information in Form 159 or CORES may result in payment not being recognized as having been received. When completing FCC Form 159 or CORES, enter the Account Number in block number 23A (call sign/other ID), enter the letters "FORF" in block number 24A (payment type code), and enter in block number 11 the FRN(s) captioned above

[48] 47 U.S.C. § 208.

[49] Debt Collection Improvement Act of 1996, Pub. L. No. 104-134, 110 Stat. 1321, 1358 (Apr. 26, 1996).

[50] For questions regarding payment procedures, please contact the Financial Operations Group Help Desk by phone at 1-877-480-3201 (option #6).

[51] FCC Form 159 is accessible at https://www.fcc.gov/licensing-databases/fees/fcc-remittance-advice-form-159.

[52] Information completed using the Commission's Registration System (CORES) does not require the submission of an FCC Form 159. CORES is accessible at https://apps.fcc.gov/cores/userLogin.do.

(Payor FRN).[53] For additional detail and wire transfer instructions, go to https://www.fcc.gov/licensing-databases/fees/wire-transfer.

- Payment by credit card must be made by using CORES at https://apps.fcc.gov/cores/userLogin.do. To pay by credit card, log-in using the FCC Username associated to the FRN captioned above. If payment must be split across FRNs, complete this process for each FRN. Next, select "Manage Existing FRNs | FRN Financial | Bills & Fees" from the CORES Menu, then select FRN Financial and the view/make payments option next to the FRN. Select the "Open Bills" tab and find the bill number associated with the CD Acct. No. The bill number is the CD Acct. No. with the first two digits excluded (e.g., CD 1912345678 would be associated with FCC Bill Number 12345678). After selecting the bill for payment, choose the "Pay by Credit Card" option. Please note that there is a $24,999.99 limit on credit card transactions.
- Payment by ACH must be made by using CORES at https://apps.fcc.gov/cores/userLogin.do. To pay by ACH, log in using the FCC Username associated to the FRN captioned above. If payment must be split across FRNs, complete this process for each FRN. Next, select "Manage Existing FRNs | FRN Financial | Bills & Fees" on the CORES Menu, then select FRN Financial and the view/make payments option next to the FRN. Select the "Open Bills" tab and find the bill number associated with the CD Acct. No. The bill number is the CD Acct. No. with the first two digits excluded (e.g., CD 1912345678 would be associated with FCC Bill Number 12345678). Finally, choose the "Pay from Bank Account" option. Please contact the appropriate financial institution to confirm the correct Routing Number and the correct account number from which payment will be made and verify with that financial institution that the designated account has authorization to accept ACH transactions.

33. **Event of Default**. AT&T agrees that an Event of Default shall occur upon the failure by AT&T to pay the full amount of the Civil Penalty on or before the due date specified in this Consent Decree.

34. **Interest, Charges for Collection, and Acceleration of Maturity Date**. After an Event of Default has occurred under this Consent Decree, the then unpaid amount of the Civil Penalty shall accrue interest, computed using the U.S. Prime Rate in effect on the date of the Event of Default plus 4.75%, from the date of the Event of Default until payment in full. Upon an Event of Default, the then unpaid amount of the Civil Penalty, together with interest, any penalties permitted and/or required by the law, including but not limited to 31 U.S.C. § 3717 and administrative charges, plus the costs of collection, litigation, and attorneys' fees, shall become immediately due and payable, without notice, presentment, demand, protest, or notice of protest of any kind, all of which are waived by AT&T.

35. **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[54] relating to the matters addressed in this Consent Decree.

36. **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

[53] Instructions for completing the form may be obtained at http://www.fcc.gov/Forms/Form159/159.pdf.

[54] *See* 5 U.S.C. § 504; 47 CFR §§ 1.1501–1.1530.

containing the particular unenforceable provision or provisions, and the rights and obligations of the Parties shall be construed and enforced accordingly.

37. **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.

38. **Subsequent Rule or Order**. The Parties agree that, if any provision of this Consent Decree conflicts with any subsequent Rule or Order adopted by the Commission, such Rule or Order shall take precedence, provided that such Rule or Order becomes and is effective, but excluding any Order specifically intended to revise the terms of this Consent Decree to which AT&T does not expressly consent.

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

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

41. **Modifications**. This Consent Decree cannot be modified without the advance written consent of both Parties.

42. **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.

43. **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.

44. **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.

_____
Loyaan A. Egal
Chief
Enforcement Bureau

_____
Date

_____
Andy Markus
Senior Vice President – Data & Artificial Intelligence, Chief Data Officer
AT&T Services, Inc.

_____
Date