Before the
Federal Communications Commission
Washington, DC 20554

In the Matter of	)	
	)	File No.: EB-IHD-14-00017829
Cox Communications, Inc.	)	Acct. No.: 201632080001
	)	FRN: 0001834696

ORDER

Adopted: November 5, 2015 **Released: November 5, 2015**

By the Chief, Enforcement Bureau:

1. Consumers of cable and satellite services are entitled to have their personal information protected. The Communications Act already imposes heightened obligations on cable and satellite operators to protect the personally identifiable information of their subscribers, and to take such actions as are necessary to prevent unauthorized access to this information. Inadequate security of subscribers' personal information can result in real world consequences for those customers, who are put at risk of financial and digital identity theft. In the wrong hands, a customer's sensitive personal information could also be used to take control of a customer's real accounts, to change the passwords on those accounts, to expose the customer's personal information on the web, and to harass or embarrass the customer through social media. Today, the Enforcement Bureau (Bureau) of the Federal Communications Commission has entered into a Consent Decree to resolve its investigation into whether Cox Communications, Inc. (Cox), failed to properly protect the confidentiality of its customers' proprietary information (PI), proprietary network information (CPNI), and personally identifiable information, and whether Cox failed to promptly notify law enforcement authorities of security breaches involving CPNI, as required by Commission rules (Rules).

2. Cox's electronic data systems were breached in August 2014 when a third party used a common social engineering ploy known as pretexting. Specifically, the third party pretended to be from Cox's information technology department and gained access to data systems containing Cox customer information by convincing a Cox customer service representative and a Cox contractor to enter their respective account IDs and passwords into a fake website, which the third party controlled. The relevant data systems did not have technical safeguards, such as multi-factor authentication, to prevent the compromised credentials from being used to access the PI and CPNI of Cox's customers. Thus, the third party was able to make use of the credentials to view personal data of Cox's current and former customers, including sensitive personal information such as name, home address, email address, phone number, partial Social Security Number, partial driver's license number, and telephone customers' account-related data. This third-party hacker then posted some of the personal information of at least eight of the affected customers on social media sites, changed the passwords of at least 28 of the affected customers, and shared customer personal information with another alleged hacker. Cox did not report the breaches through the Commission's breach-reporting portal.

3. Congress and the Commission have made clear that cable operators such as Cox must "take such actions as are necessary to prevent unauthorized access to such information by a person other than the subscriber or cable operator."[1] Furthermore, telecommunications carriers such as Cox must take

[1] 47 U.S.C. § 551(c)(1); *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, Notice of Proposed Rulemaking, 11 FCC Rcd 12513, 12525 para. 24 n.61 (1996) ("[I]n the Cable Communications Policy Act of 1984, Congress . . . sought to restrict unauthorized use of personably identifiable information [PII] by cable operators.").

"every reasonable precaution"[2] to protect their customers' data. In addition, the law requires carriers to promptly disclose CPNI breaches via our reporting portal within seven (7) business days after reasonable determination of a breach to facilitate the investigations of the FBI and the United States Secret Service.[3]

4. To settle this matter, Cox will pay a civil penalty of $595,000 and develop and implement a compliance plan to ensure appropriate processes and procedures are incorporated into Cox's business practices to protect consumers against similar data breaches in the future. In particular, Cox will be required to improve its privacy and data security practices by: (i) designating a senior corporate manager who is a certified privacy professional; (ii) conducting privacy risk assessments; (iii) implementing a written information security program; (iv) maintaining reasonable oversight of third party vendors, to include implementing multi-factor authentication; (v) implementing a more robust data breach response plan; and (vi) providing privacy and security awareness training to employees and third-party vendors. Cox will also identify all affected consumers, notify them of the breach, provide them with free credit monitoring, and file regular compliance reports with the FCC.

5. 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 Cox's compliance with Sections 201(b), and 222(a) and (c), and 631(c) of the Communications Act of 1934, as amended (Act), as well as Sections 64.2010(a) and 64.2011(b) of the Rules.[4]

6. In the absence of material new evidence relating to this matter, we do not set for hearing the question of Cox's basic qualifications to hold or obtain any Commission license or authorization.[5]

7. Accordingly, **IT IS ORDERED** that, pursuant to Section 4(i) of the Act[6] and the authority delegated by Sections 0.111 and 0.311 of the Rules,[7] the attached Consent Decree **IS ADOPTED** and its terms incorporated by reference.

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

The Cable Act generally prohibits the disclosure of PII unless such disclosure is necessary to render the services requested or for a legitimate business activity related to such service. *See* 47 U.S.C. § 551**(**c)(2)(A). *See also id.* §§ 201, 222(a), (c); 47 C.F.R. § 64.2010.

[2] *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, para. 64 (2007).

[3] *See* 47 C.F.R. § 64.2011(b).

[4] *See* 47 U.S.C. §§ 201, 222(a), (c); 47 C.F.R. §§ 64.2010, 64.2011.

[5] *See* 47 C.F.R. § 1.93(b).

[6] 47 U.S.C. § 154(i).

[7] 47 C.F.R §§ 0.111, 0.311.

9. **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 Barry Ohlsohn, Esq., Vice President, Regulatory Affairs, Cox Enterprises, Inc., 975 F Street, NW, Suite 300, Washington, DC 20004, and to counsel David H. Solomon, Esq., and J. Wade Lindsay, Esq., Wilkinson Barker Knauer, LLP, 1800 M Street, N.W., Suite 800N, Washington, D.C. 20036.

FEDERAL COMMUNICATIONS COMMISSION

Travis LeBlanc
Chief
Enforcement Bureau

Before the
Federal Communications Commission
Washington, DC 20554

In the Matter of	)	File No.: EB-IHD-14-00017829
	)	Account No.: 201632080001
Cox Communications, Inc.	)	FRN: 0001834696

CONSENT DECREE

1. The Enforcement Bureau of the Federal Communications Commission and Cox Communications, Inc. (Cox), by their authorized representatives, hereby enter into this Consent Decree for the purpose of terminating the Enforcement Bureau's investigation into whether Cox violated Sections 201(b) and 222(a) and (c), and 631 of the Communications Act of 1934, as amended, and Sections 64.2010(a) and 64.2011(b) of the Commission's rules.[1]

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.[2]

(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 Customer whose PI and/or CPNI was viewed by unauthorized third parties in connection with the August 7, 2014, data breach.

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

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

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

(g) "Compliance Officer" means the individual designated in paragraph 16 of this Consent Decree as the person responsible for administration of the Compliance Plan.

(h) "Compliance Plan" means the compliance obligations, programs, and procedures described in this Consent Decree at paragraph 17.

(i) "Covered Employees" means all employees of Cox assigned to call centers that provide customer service or sales service for Cox Customers managed and operated by Cox, Cox field technicians, and Cox information technology Help Desk employees, who perform or directly supervise, oversee, or manage the performance of, duties that involve access to, use, or disclosure of PI and/or CPNI. Covered Employees do not include Covered Third Party Employees.

(j) "Covered Third Party" means any third-party that, on behalf of Cox, operates and/or manages a call center that provides customer service or sales service for Cox,

[1] 47 U.S.C. §§ 201(b), 222(a) and (c), 551; 47 C.F.R. §§ 64.2010(a) and 64.2011(b).

[2] 47 U.S.C. § 151 *et seq.*

provides field technician services, or provides information technology Help Desk services.

(k) "Covered Third Party Employees" means all employees of Covered Third Parties assigned to call centers that provide customer service to Cox Customers, field technicians, and information technology Help Desk employees, who perform or directly supervise, oversee, or manage the performance of duties that involve access to, use, or disclosure of PI and/or CPNI of Cox Customers.

(l) "Cox" means Cox Communications, Inc., its wholly owned subsidiaries that own and operate cable systems that provide video, broadband, or telecommunications services in the United States and successors-in-interest.

(m) "Customer" means any current and/or former subscriber of any Cox service, which service is subject to the Communications Laws. "Customer" shall include any applicant for any Cox service to the extent that Cox, or any Covered Third Party collects and stores PI and/or CPNI regarding the applicant on behalf of Cox, in any Cox or Covered Third Party electronic data systems.

(n) "Customer Proprietary Network Information" or "CPNI" shall have the meaning set forth at 47 U.S.C. § 222(h).

(o) "Effective Date" means the date by which the Bureau and Cox have signed the Consent Decree.

(p) "Investigation" means the investigation commenced by the Bureau in File No. EB-IHD-14-00017829 regarding whether Cox violated the Privacy Laws in 2014.[3]

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

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

(s) "Personal Information" or "PI" 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

[3] *See, e.g.*, Letter from Jeffrey J. Gee, then-Acting Chief, Investigations and Hearings Division, Enforcement Bureau to Barry J. Ohlson, Esq., Vice President, Regulatory Affairs, Cox Enterprises, Inc., (Feb. 12, 2015) (on file in EB-IHD-14-00017829). Cox responded to that letter and subsequent requests for information, and Cox requested confidential treatment of specified information contained in its responses (including material contained in the accompanying exhibits) pursuant to Sections 0.457 and 0.459 of the Rules. *See* 47 C.F.R. §§ 0.457, 0.459. Letter from David H. Solomon and J. Wade Lindsay, Attorneys for Cox, to Jennifer A. Lewis, Investigations and Hearings Division, Enforcement Bureau, Federal Communications Commission (Mar. 16, 2015) (on file in EB-IHD-14-00017829) (LOI Response); Letter from David H. Solomon and J. Wade Lindsay, Attorneys for Cox Communications, to Marlene H. Dortch, Secretary, Federal Communications Commission (May 4, 2015) (on file in EB-IHD-14-00017829) (Supplemental LOI Response); Letter from David H. Solomon and J. Wade Lindsay, Attorneys for Cox Communications, to Marlene H. Dortch, Secretary, Federal Communications Commission (May 20, 2015) (on file in EB-IHD-14-00017829). Because we do not disclose material Cox identified as confidential, we defer ruling on the requests unless and until necessary. *See* 47 C.F.R. § 0.459(d)(3) (permitting deferred rulings until a request for inspection has been made pursuant to Sections 0.460 or 0.461 of the Rules; such materials will be accorded confidential treatment until the Commission acts on such requests and all subsequent appeal and stay proceedings have been exhausted).

card number, in combination with any required security code, access code, PIN, 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) "Privacy Laws" means Sections 47 U.S.C. §§ 201(b), 222, and 551, and 47 C.F.R §§ 64.2001-2011, insofar as they relate to the security, confidentiality, and integrity of PI and/or CPNI.

(u) "Rules" means the Commission's regulations found in Title 47 of the Code of Federal Regulations.

II. BACKGROUND

3. Section 631(c) of the Act provides that, with certain exceptions, a cable operator "shall not disclose personally identifiable information concerning any subscriber without the prior written or electronic consent of the subscriber concerned and shall take such actions as are necessary to prevent unauthorized access to such information by a person other than the subscriber or cable operator."[4]

4. Section 222 of the Act is entitled "Privacy of customer information."[5] Section 222(a), entitled "In general," provides that "[e]very telecommunications carrier has a duty to protect the confidentiality of proprietary information of, and relating to . . . customers."[6] The Commission has interpreted Section 222(a) as applying to customer "proprietary information" that does not fit within the statutory definition of CPNI.[7] The Commission has stated that proprietary information broadly encompasses all types of information that should not be exposed widely to the public, whether that information is sensitive for economic or personal privacy reasons,[8] and that this includes privileged information, trade secrets, and personally identifiable information.[9]

5. Section 222(c) of the Act imposes certain restrictions on telecommunications carriers to protect the confidentiality of their customers' CPNI.[10] Section 64.2010(a) of the Rules establishes protections for CPNI by requiring carriers to take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI.[11] Section 64.2011(b) requires carriers to provide notification of a CPNI breach via the FCC portal "[a]s soon as practicable, and in no event later than seven (7) business days, after reasonable determination of the breach."[12]

6. Section 201(b) of the Act states, in pertinent part, that "[a]ll charges, practices, classifications, and regulations for and in connection with [interstate or foreign] communication service

[4] 47 U.S.C. § 551(c)(1).

[5] *See id*. § 222.

[6] *Id.* § 222(a).

[7] *See, e.g., Terracom Inc. and YourTel America, Inc.*, Notice of Apparent Liability for Forfeiture, 29 FCC Rcd 13325, 13330-13332, paras. 14-19 (2014) (citing *Lifeline and Link Up Reform and Modernization*, Report and Order and Further Notice of Proposed Rulemaking, 27 FCC Rcd 6656, 6745 para. 207 (2012)) (*Terracom NAL*), *settled by TerraCom, Inc. and YourTel America, Inc*., Order and Consent Decree, 30 FCC Rcd 7075 (Enf. Bur. 2015).

[8] *Id*.

[9] *Id*. at 13331, para. 17.

[10] *See* 47 U.S.C. § 222(c).

[11] *See* 47 C.F.R. § 64.2010(a).

[12] *Id.* § 64.2011(b).

[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."[13] The Commission has interpreted Section 201(b) to apply to carriers' data-security practices for protecting proprietary information.[14] In that regard, the Commission has interpreted Section 201(b) to require companies to employ just and reasonable data security practices to protect consumers' proprietary information.[15]

7. Cox provides digital cable television services, broadband Internet access service, telecommunications services, and home automation services in the United States. Cox is the third largest cable company in the United States, serving approximately six million residential and commercial customers,[16] and is the seventh largest landline telephone provider in the United States.[17]

8. The Bureau's review of the record shows that Cox's systems were breached on or about August 7, 2014, by a hacker using the alias "EvilJordie," a member of the hacker group known as the Lizard Squad.[18] This individual apparently used a social engineering method known as pretexting[19] to gain access to Cox electronic data systems containing customer information. Specifically, EvilJordie pretended to be from Cox's information technology department and convinced a contractor to enter her account ID and password into a fake, or "phishing," website on or about August 7, 2014.[20] According to Cox, the phony phishing website appeared to be a Cox website but, in fact, was controlled by "EvilJordie."[21] Around the same time, the access credentials of a Cox Tech Support representative were also compromised by means of a social engineering effort that prompted the representative to enter his access credentials into the same phishing website. Cox states that it believes that "EvilJordie" shared the compromised credentials with "chF."[22]

9. As a result of these actions, the hackers had access to Cox electronic data systems that included some PI of [redacted] active Customers and some PI and CPNI of [redacted] telephone

[13] 47 U.S.C. § 201(b).

[14] *Terracom NAL*, 29 FCC Rcd at 13335–36, paras. 31–32.

[15] *Id.*

[16] Cox Communications Fact Sheet, http://newsroom.cox.com/company-overview (last visited Nov. 3, 2015).

[17] *See* Cox Communications Digital Telephone Fact Sheet, http://newsroom.cox.com/product-fact-sheets (last visited Nov. 3, 2015).

[18] *See* LOI Response at 1-2, 8-10.

[19] "Pretexting" is a form of misrepresentation whereby the perpetrator adopts the identity of a legitimate person or entity to obtain confidential and personal information belonging to the targeted individual. *See* Federal Bureau of Investigation, "Owner, Employee, and Contractor of Private Investigative Firm Sentenced in Connection with Pretexting" (Dec. 14, 2012), https://www.fbi.gov/sanfrancisco/press-releases/2012/owner-employee-and-contractor-of-private-investigative-firm-sentenced-in-connection-with-pretexting.

[20] *See* LOI Response at 1-2, 8-9. "Phishing" is the deceptive use of an identity that appears to come from a legitimate, well-known source in order to trick an individual into divulging sensitive or personal information, such as account numbers or passwords, often through a link to a copycat of the purported source's Web site. *See* Federal Trade Commission, FTC Issues Staff Report on Roundtable Discussion About Phishing Education (Jul. 14, 2008), https://www.ftc.gov/news-events/press-releases/2008/07/ftc-issues-staff-report-roundtable-discussion-about-phishing.

[21] LOI Response at 1-2, 8-9.

[22] *See* LOI Response at 1-2, 8-10. The Bureau's review of the record also shows that a single Cox subscriber reported a possible incident by a hacker using the alias "chF," (an apparent member of the Lizard Squad) to Cox on July 22 and 31, 2014. *See, e.g.*, LOI Response at Bates # 00643-48, 01640-41.

Customers.[23] The record reflects that from August 7, 2014, through August 14, 2014, the hackers viewed some PI of 54 current Affected Customers, seven former Affected Customers, and likely viewed some CPNI of at least one, but possibly up to four, of these Affected Customers.[24] The hackers posted some information of eight of the Affected Customers on social media sites; they also changed the passwords of 28 of the Affected Customers' whose PI was viewed.[25] Of the current Affected Customers whose information was viewed, 20 subscribed to telephone service at the time of the breach.[26]

10. Cox asserts that it learned of the August 7th breach on August 12, 2014, when a Cox employee in San Diego received an email from a Nevada Customer who complained of account information being posted on a social media site.[27] Cox's privacy team then engaged its customer safety team, which investigated the incident, identified the source of the breach, and disabled the compromised access credentials within two days of learning of the August 7th breach. At the time of the breach, Cox employed multi-factor authentication for some employees and third party contractors with access to Cox electronic data systems, but not for the compromised employee or contractor. Cox's internal policies and training programs expressly prohibited Cox employees and third party contractors from disclosing access credentials to anyone and warned against pretexting attacks. On August 18, 2014, Cox directly contacted the FBI and cooperated in the subsequent investigation of the breach, which resulted in the arrest of "EvilJordie."[28] Cox did not disclose the CPNI breach via the FCC data breach reporting portal. Via a letter dated September 16, 2014, Cox notified all but two of current Affected Customers that their PI/CPNI had been compromised as a result of a Cox customer service representative sharing access credentials with an unknown individual and offered free credit monitoring services.[29] Cox took other remedial steps as a result of the incident.

11. The Bureau subsequently commenced an investigation that it states involved whether Cox: (i) failed to properly protect the confidentiality of Customers' personally identifiable information; (ii) failed to take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI; (iii) failed to provide timely notification to law enforcement of a CPNI breach; and (iv) engaged in unjust and unreasonable practices by (a) failing to employ reasonable data security practices to protect proprietary information and CPNI, and failing to monitor for Customers' breached data online; and (b) failing to notify all potentially affected Customers of the breaches. The Parties negotiated the following terms and conditions of settlement and hereby enter into this Consent Decree as provided below.

III. TERMS OF AGREEMENT

12. **Adopting Order**. The provisions of this Consent Decree shall be incorporated by the Bureau in an Adopting Order without change, addition, deletion, or modification.

13. **Jurisdiction**. Cox 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.

[23] *See* Supplemental LOI Response at 8-9.

[24] *See* LOI Response at 2; Supplemental LOI Response at 10. No credit card information could have been viewed and only the last four digits of the Social Security number and driver's license number, not the entire Social Security or driver's license number, could have been viewed. LOI Response at 11; Supplemental LOI Response at 8-9.

[25] *See* Supplemental LOI Response at 2.

[26] *Id*.

[27] *See* LOI Response at 9-10.

[28] *See id*. at 9-10; 17-18.

[29] *See id*. at 14.

14. **Effective Date**. 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.

15. **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, Cox 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, on its own motion, any new proceeding, formal or informal, or take any action on its own motion against Cox concerning the matters that were the subject of the Investigation. The Bureau also 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 on its own motion any proceeding, formal or informal, or to designate for hearing the question of Cox's basic qualifications to be a Commission licensee or hold Commission licenses or authorizations.[30]

16. **Compliance Officer**. Within thirty (30) calendar days after the Effective Date, Cox 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, together with the Chief Privacy Officer (who shall be privacy certified by an industry-certifying organization and who shall keep current through appropriate continuing privacy education courses) and Chief Information Security Officer, shall be responsible for developing, implementing, and administering the Compliance Plan, including the Information Security Program (as defined in paragraph 17(b)) required under the Compliance Plan, and ensuring that Cox 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, Chief Information Security Officer, or managers reporting to either the Compliance Officer or Chief Information Security Officer with responsibilities related to this Consent Decree, 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 the Privacy Laws relevant to their duties, prior to assuming their duties.

17. **Compliance Plan**. For purposes of settling the matters set forth herein, Cox agrees that it shall, within one hundred twenty (120) calendar days after the Effective Date, supplement its existing compliance policies and procedures regarding the Privacy Laws by developing and implementing a Compliance Plan designed to ensure future compliance with the Privacy Laws, and with the terms and conditions of this Consent Decree, which shall be implemented and operated in accordance with Cox's risk-based approach. Such Compliance Plan must include the following components:

(a) **Risk Assessment**. Cox shall conduct a comprehensive and thorough risk assessment, conducted with reference to the NIST Cybersecurity Framework, to identify internal and external risks to the security, confidentiality, and integrity of PI/CPNI collected or maintained by Cox or Covered Third Parties that could result in unauthorized access, disclosure, misuse, destruction, or compromise of such information (Risk Assessment). The Risk Assessment, which shall be completed no later than December 31, 2016, must evaluate in writing the likelihood and potential impact of these threats and the sufficiency of existing policies, procedures, and other safeguards in place to control risks. Additional Risk Assessments shall be conducted at least biennially and Cox shall notify the Commission of completion of the Risk Assessments within thirty (30) calendar days via e-mail to the persons listed in paragraph 19(d).

[30] *See* 47 C.F.R. § 1.93(b).

(b) **Information Security Program**. Within one hundred fifty (150) calendar days after the Effective Date, Cox shall review and revise as appropriate its information security program to ensure that, using a risk-based approach, it has a reasonable and comprehensive security program to protect the security, confidentiality, and integrity of PI and CPNI collected and/or maintained by Cox or Covered Third Parties (Information Security Program). Cox shall ensure that such Information Security Program is documented in writing (including, as appropriate, within the Operating Procedures and Compliance Manual described below) and includes:

i. Administrative, technical, and physical safeguards that are reasonable in light of Cox's size and complexity, the nature and scope of Cox's activities, the sensitivity of the PI/CPNI collected or maintained by or on behalf of Cox, and the risks identified through risk assessments, including the use of multiple factor authentication or equivalent control(s) for Covered Employees' access to PI/CPNI;

ii. Reasonable measures to protect PI/CPNI collected or maintained by Covered Third Parties, including exercising due diligence in selecting Covered Third Parties, where reasonably feasible requiring Covered Third Parties by contract (upon execution of new agreements and renewal agreements) to implement and maintain reasonable and comprehensive safeguards of both the physical and electronic protection of PI/CPNI equivalent to the safeguards used by Covered Employees (e.g., with regard to multiple factor access/authentication or equivalent control(s) to Cox data systems/Customer information), engaging in appropriate verification of Covered Third Parties' compliance with their security obligations, and implementing appropriate measures to sanction Covered Third Parties that fail to comply with their security obligations (including, where appropriate, terminating Cox's relationship with such Covered Third Parties); and

iii. Policies and procedures to properly identify the nature and extent of CPNI and PI collected or maintained by Cox and Covered Third Parties, minimize the number of Employees who have access to PI and CPNI on a strictly need-to-know basis tied to job functions, collect the minimum amount of PI necessary to provision and provide services, and collect and maintain PI in a manner that is secure.

In addition, and in accordance with its risk-based approach, Cox shall:

iv. Review and evaluate periodically the effectiveness of the Information Security Program's key controls, systems, and procedures particularly with regard to how such controls, systems, and procedures impact compliance with the Privacy Laws;

v. Monitor critical points within Cox's infrastructure containing PI and CPNI for security events. This process includes taking information feeds from industry sources and internal detection tools (e.g., antivirus) and correlating these information sources to alert Cox's security monitoring center when a potential event has occurred. The security monitoring team will take action on alerts as necessary;

vi. Adjust and update its Information Security Program as appropriate in light of limitations and deficiencies indicated by the reviews, evaluations, and monitoring described herein; and

vii. Conduct annual audits of selected call center systems and processes using procedures and standards generally accepted in the profession, to ensure compliance with the Privacy Laws and this Consent Decree. The audits may be performed by Cox Enterprises Inc.'s Audit Services team (which operates separately from Cox) and which itself and through a co-sourcing relationship with a large global external audit firm, which Cox represents has the requisite knowledge and information-security related certifications including but not limited to: Certified Information Security Auditor; Certified Information Systems Security Professional; Certified Privacy Technologist; Certified Risk and Information Systems Control; Certified Fraud Examiner; and Certified Internal Auditor. Systems and processes shall be selected for audit based on Cox's risk evaluations and prioritization. Cox will notify the Commission of the completion of the audits within thirty (30) days via e-mail to the persons listed in paragraph 19(d).

viii. Conduct annual penetration testing of selected systems and processes related to payment cards and collection and storage of PI/CPNI. Systems and processes shall be selected for testing based on Cox's reasonable risk evaluations and prioritization.

ix. Develop an approach to internal threat monitoring that includes the detection of anomalous conduct by Covered Employees no later than December 31, 2016 and begin implementing such approach within one hundred twenty (120) days of that date.

(c) **Third Party Oversight**. Within one hundred twenty (120) calendar days after the completion of the Information Security Program, Cox shall implement the provisions of paragraph 17(b)(ii). In addition, Cox shall require all off-network access by Covered Third Parties with access to Cox customer PI/CPNI to be authenticated through an approved site-to-site virtual private network by December 31, 2016. Furthermore, by the first quarter of 2016, Cox shall conduct a formal assessment by a third party consulting firm to identify additional two-factor authentication opportunities, and by the end of the first quarter of 2016 shall complete the migration of all Covered Third Parties with access to Cox customer PI/CPNI leveraging remote access Citrix platforms to a two-factor authentication solution.

(d) **Incident Response Plan**. Within one hundred and twenty (120) calendar days after the Effective Date, Cox shall review, revise and maintain its Incident Response Plan to ensure that it is reasonable, comprehensive, and enables Cox to detect, respond to, and provide timely notification, in accordance with the Privacy Laws, applicable law, and the requirements of subpart 17(e) below, to all relevant Customers and relevant governmental authorities of data breaches involving PI and CPNI. Such Incident Response Plan shall contain processes to (i) identify, (ii) investigate, (iii) mitigate, (iv) remediate, and (v) review information security incidents to identify root causes and to develop improved responses to security threats. Cox shall perform annual test exercises of the Incident Response Plan, and shall subject such plan to third-party review.

(e) **Breach Notification**. Within one hundred and twenty (120) calendar days after the Effective Date, and periodically thereafter, Cox shall review its breach notification practices to ensure that, to the extent they do not already so provide, in the event of an unauthorized breach of Customer PI/CPNI, Cox shall: (i) at least to the extent required by federal or state law, or guidance from law enforcement, notify all Customers (at the Customer's last known address and pursuant to Cox's reasonable

efforts to locate the Customer) whose unredacted and/or unencrypted PI/CPNI information has been, or for which Cox knew, acquired by an unauthorized person; (ii) offer complimentary credit monitoring service for a minimum of one year to any Customer whose unredacted and/or unencrypted PI/CPNI is reasonably believed by Cox to have been acquired by an unauthorized person and if, consistent with industry practices, Cox reasonably believes involves a risk of identity theft; and (iii) conduct targeted monitoring of known websites for breach activity to identify potential Customer PI/CPNI data. Cox shall ensure that policies and statements on Cox's websites regarding the security of Customers' PI and CPNI accurately reflect Cox's data security practices, and are updated routinely to reflect any material changes.

(f) **Remediation Measures**. To the extent that Cox has not previously satisfied the requirements set forth below, within one hundred and twenty (120) calendar days after the Effective Date, unless otherwise indicated, Cox shall, with respect to the breach that was the subject of the Investigation:

i. Continue conducting targeted monitoring of known websites for breach activity to identify potential Affected Customer PI/CPNI data;

ii. Offer to provide one year of complimentary credit monitoring services to all Affected Customers through a nationally recognized credit monitoring service, the availability of which must be described in the notice discussed below; and

iii. Identify each Affected Customer and ensure that each Affected Customer has been notified (at the Customer's last known address and pursuant to Cox's reasonable efforts to locate the Customer) that his or her PI and/or CPNI was compromised. The notification to each Affected Customer must include:

a. A general description of the manner in which the Affected Customer's PI/CPNI was compromised;

b. A general description for all Affected Customers of the type of PI/CPNI that was compromised;

c. The toll-free telephone numbers and addresses of the major credit reporting agencies;

d. Information regarding the complimentary credit monitoring services available to Affected Customers;

e. A toll-free hotline or website where Affected Customers may contact Cox to inquire about their compromised PI, and receive reasonable and comprehensive counseling on responding to and mitigating credit harm incidences, including identity theft; and

f. Reasonable and comprehensive information regarding free and/or readily available credit protection options including obtaining free annual credit reports, placing fraud alerts on credit files, requesting security freezes, contacting financial institutions, and any other such free and/or readily available credit protections.

(g) **Notice of Consent Decree**. Within one hundred twenty (120) calendar days after the Effective Date, Cox shall deliver a copy of this Consent Decree to all existing Covered Employees, and shall also deliver a copy of this Consent Decree to all future Covered Employees within sixty (60) calendar days after the person assumes such

position or responsibilities. The Consent Decree can be delivered together with the Compliance Manual as provided in subpart 17(i) below.

(h) **Operating Procedures**. Within one hundred twenty (120) calendar days after the Effective Date, Cox shall establish Operating Procedures that all Covered Employees must follow to help ensure Cox's compliance with this Consent Decree, including the policies and procedures adopted pursuant to subparts (a)-(g) of this paragraph, and the Privacy Laws. Cox shall also develop a compliance checklist that describes the key steps that a Covered Employee must follow to ensure compliance with this Consent Decree and the Privacy Laws.

(i) **Compliance Manual**. Within one hundred twenty (120) calendar days after the Effective Date, Cox shall review, revise, use, and maintain a Compliance Manual (which may be in hard copy and/or electronic format). Within the same period, Cox shall distribute the Compliance Manual to all Covered Employees and to each Covered Third Party, requesting, and, where permitted by contract, requiring the Covered Third Party to distribute the Compliance Manual to each Covered Third Party Employee. For any person who becomes a Covered Employee more than one hundred twenty (120) calendar days after the Effective Date, Cox shall distribute the Compliance Manual to that person within sixty (60) calendar days after the date such person becomes a Covered Employee, and prior to such person engaging with Customers with respect to Cox's services. Further, Cox shall request, and where permitted by contract, require each Covered Third Party to distribute the Compliance Manual to each person who becomes a Covered Third Party Employee more than one hundred twenty (120) calendar days after the Effective Date within sixty (60) calendar days after such person becomes a Covered Third Party Employee, and prior to such person engaging with Customers with respect to Cox's services.

i. The Compliance Manual shall set forth and explain the requirements of the Privacy Laws and this Consent Decree, and shall instruct Covered Employees to ensure Cox's compliance with the Privacy Laws and this Consent Decree, including the policies and procedures adopted pursuant to subparts (a)-(h) of this paragraph. Cox shall request, and where permitted by contract require, Covered Third Parties to direct Covered Third Party Employees to consult and follow the Operating Procedures.

ii. The Compliance Manual shall require Covered Employees to contact their supervisor or the Compliance Officer with any questions or concerns that arise with respect to Cox's obligations under or compliance with the Privacy Laws and this Consent Decree, and require any supervisor who receives such information from a Covered Employee or Covered Third Party Employee to promptly notify the Compliance Officer. Cox shall request, and where permitted by contract require, Covered Third Parties to provide appropriate mechanisms for Covered Third Party Employees to contact their supervisor with any questions or concerns that arise with respect to their obligations under or compliance with the Privacy Laws and this Consent Decree, and for any such supervisor who receives such information from a Covered Third Party Employee to promptly notify the Compliance Officer. Cox shall provide and request, and, where permitted by contract, require Covered Third Parties to provide a hotline or other appropriate mechanism for anonymous reporting of any noncompliance.

iii. Cox shall review and revise the Compliance Manual to ensure that the information set forth therein remains current and complete.

iv. Cox shall distribute any revisions of the Compliance Manual to all Covered Employees and Covered Third Parties within sixty (60) calendar days after any revisions have been made by Cox. These revisions may be in electronic format.

(j) **Compliance Training Program**. Within six months after the Effective Date, Cox shall review, revise, implement, and maintain a compliance training program to ensure compliance with the Privacy Laws and this Consent Decree. In addition, Cox shall request, and where permitted by contract, require all Covered Third Parties to ensure that their Covered Third Party Employees receive training in accordance with the Compliance Training Program:

i. The Compliance Training Program shall include reasonable and comprehensive privacy and security awareness training for all Covered Employees. The program shall include instruction on Cox's obligations, policies, and procedures for protecting PI and CPNI pursuant to the Privacy Laws and this Consent Decree, including identifying and collecting PI from Customers, recognizing security threats and suspicious activity that may indicate that PI has been compromised, the timely reporting of data breaches, and other reasonable and appropriate training regarding the protection of PI and CPNI. Cox shall cause all Covered Employees whose job functions relate to the implementation of the remediation measures described in paragraph 17(f) to receive training regarding such remediation measures, as described below. For purposes of complying with the provisions of this paragraph, Cox is permitted to provide the training or use a third party to provide the training described herein.

ii. As part of the Compliance Training Program, Cox shall ensure that each Covered Employee is advised of Cox's obligations to report any noncompliance with the Privacy Laws and this Consent Decree, and is instructed on how to disclose noncompliance to the Compliance Officer, including instructions on how to anonymously report such noncompliance. Cox shall request, and where permitted by contract, require, Covered Third Parties to disseminate the same instructions to each Covered Third Party Employee.

iii. Cox shall ensure that the training for Covered Employees is conducted pursuant to the Compliance Training Program within six (6) months after the Effective Date, except that any person who becomes a Covered Employee at any time after the initial Compliance Training Program shall be trained within sixty (60) calendar days after the date such person becomes a Covered Employee. Cox shall document its Covered Employees' completion of the training. Cox shall request, and where permitted by contract, require all Covered Third Parties to conduct the same type of training for each of their Covered Third Party Employees within the same period, and to document completion of that training.

iv. Within one hundred eighty (180) calendar days after the Effective Date, Cox shall not allow any Covered Employee to interact with any Customer about Cox's service until the Covered Employee has been

trained and has received a copy of the Compliance Manual. Beginning within one hundred eighty (180) calendar days after the Effective date, Cox shall further request, and where permitted by contract, require all Covered Third Parties to ensure that their Covered Third Party Employees shall not interact with any Customer about Cox's service until their Covered Third Party Employees have been trained consistent with this subparagraph 17(j); and

v. Cox shall ensure that the Compliance Training Program is conducted at least annually for Covered Employees. Cox shall request, and where permitted by contract, require Covered Third Parties to ensure that the Compliance Training Program is conducted at least annually for Covered Third Party Employees. Cox shall periodically review and revise the Compliance Training Program as necessary to ensure that it remains current and complete and to enhance its effectiveness.

18. **Reporting Noncompliance**. Cox shall report any material noncompliance with the Privacy Laws, and the terms and conditions of this Consent Decree, within fifteen (15) calendar days after discovery by the Compliance Officer, Chief Information Security Officer, or managers reporting to either the Compliance Officer or Chief Information Security Officer with responsibilities related to this Consent Decree, of such noncompliance. Such reports shall include a detailed explanation of: (i) each known instance of noncompliance; (ii) the steps that Cox has taken or will take to remedy such noncompliance; (iii) the schedule on which such remedial actions will be taken; and (iv) the steps that Cox has taken or will take to prevent the recurrence of any such noncompliance. Cox shall also report to the FCC any breaches of PI or CPNI involving any Covered Employees or Covered Third Party Employees that Cox 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 Cox submitted to the applicable Federal and 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 or PI/CPNI breaches shall be submitted to the Chief, Investigations and Hearings Division, Enforcement Bureau, Federal Communications Commission, 445 12th Street, SW, Rm. 4-C321, Washington, DC 20554, with a copy submitted electronically to David.Roberts@fcc.gov, Kenneth.Scheibel@fcc.gov, Jennifer.Lewis@fcc.gov, and Dana.Leavitt@fcc.gov.

19. **Compliance Reports**. Cox 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 Cox's efforts during the relevant period to comply with the terms and conditions of this Consent Decree and the Privacy Laws. In addition, each Compliance Report shall include a certification by the Compliance Officer, as an agent of and on behalf of Cox, stating that the Compliance Officer has personal knowledge that Cox: (i) has established and implemented the Compliance Plan required by paragraph 17; (ii) has utilized the applicable Operating Procedures 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 18 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.[31]

(c) If the Compliance Officer cannot provide the requisite certification, the Compliance Officer, as an agent of and on behalf of Cox, shall provide the Commission with a detailed explanation of the reason(s) why and describe fully: (i) each instance of such noncompliance; (ii) the steps Cox 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 Cox has taken or will take to prevent the 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, Investigations and Hearings Division, Enforcement Bureau, Federal Communications Commission, 445 12th Street, SW, Rm. 4-C321, Washington, DC 20554, with copies submitted electronically to Jennifer.Lewis@fcc.gov, Dana.Leavitt@fcc.gov, Kenneth.Scheibel@fcc.gov, and David.Roberts@fcc.gov.

20. **Termination Date**. Unless stated otherwise, the obligations set forth in paragraphs 18 and 19 of this Consent Decree shall expire thirty-six (36) months after the Effective Date. The obligations set forth in paragraphs 16, 17(a) and 17(b) shall expire seven (7) years after the Effective Date. The obligations set forth in paragraphs 17(c)-(j) shall expire six (6) years after the Effective Date.

21. **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[32] against Cox 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 Cox with the Communications Laws.

22. **Civil Penalty**. Cox shall pay a civil penalty to the United States Treasury in the amount of Five Hundred Ninety-five Thousand dollars ($595,000.00) (Civil Penalty). Cox shall send electronic notification of payment to Investigations and Hearings Division, Enforcement Bureau, Federal Communications Commission at Jeffrey.Gee@fcc.gov, David.Roberts@fcc.gov, Kenneth.Scheibel@fcc.gov, Jennifer.Lewis@fcc.gov, and Dana.Leavitt@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.[33] 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.

[31] *See* 47 C.F.R. § 1.16.

[32] 47 U.S.C. § 208.

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

- 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.

23. **Waivers**. As of the Effective Date, Cox 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. Cox 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 Cox nor the Commission shall contest the validity of the Consent Decree or the Adopting Order, and Cox shall waive any statutory right to a trial *de novo*. Cox hereby agrees to waive any claims it may otherwise have under the Equal Access to Justice Act[34] relating to the matters addressed in this Consent Decree.

24. **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.

25. **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.

26. **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 Cox does not expressly consent) that provision will be superseded by such Rule or Order.

27. **Limitation**. The definitions and terms set out in this Consent Decree are intended solely for this Consent Decree and not as an extension or limitation of the Privacy Laws.

28. **Successors and Assigns**. Cox agrees that the provisions of this Consent Decree shall be binding on its successors, assigns, and transferees.

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

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

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

31. **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.

32. **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.

33. **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

_____

Jennifer W. Hightower
Senior Vice President and General Counsel
Cox Communications, Inc.

_____

Date