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

In the Matter of	)	File No.: EB-TCD-13-00009175
	)	
TerraCom, Inc. and YourTel America, Inc.	)	NAL/Acct. No.: 201432170015
	)	
Apparent Liability for Forfeiture	)	FRNs: 0010103745 and 0020097572

NOTICE OF APPARENT LIABILITY FOR FORFEITURE

Adopted: October 24, 2014 **Released: October 24, 2014**

By the Commission: Chairman Wheeler and Commissioner Clyburn issuing separate statements; Commissioners Pai and O'Reilly dissenting and issuing separate statements.

I. INTRODUCTION

1. The Commission is committed to protecting the sensitive personal information of American consumers from misappropriation, breach, and unlawful disclosure. Today, we take action against two companies that collected names, addresses, Social Security numbers, driver's licenses, and other proprietary information (PI) belonging to low-income Americans and stored them on unprotected Internet servers that anyone in the world could access with a search engine and basic manipulation. The companies stored such consumer PI in two publicly accessible folders on the Internet without password protection or encryption. By not employing appropriate or even reasonable security measures, the companies exposed their customers to an unacceptable risk of identity theft and other serious consumer harms.

2. We find that TerraCom, Inc. (TerraCom) and YourTel America, Inc. (YourTel) (collectively, the Companies) apparently willfully and repeatedly violated the law when they allegedly: (i) failed to properly protect the confidentiality of consumers' PI they collected from applicants for the Companies' wireless and wired Lifeline telephone services; (ii) failed to employ reasonable data security practices to protect consumers' PI; (iii) engaged in deceptive and misleading practices by representing to consumers in the Companies' privacy policies that they employed appropriate technologies to protect consumers' PI when, in fact, they had not; and (iv) engaged in unjust and unreasonable practices by not fully informing consumers that their PI had been compromised by third-party access. Based on our review of the facts and circumstances surrounding these apparent violations of Sections 201(b) and 222(a) of the Communications Act of 1934, as amended (Communications Act or Act) and our rules, we propose a forfeiture of $10,000,000.

II. BACKGROUND

3. Both TerraCom and YourTel are common carriers providing telecommunications services as part of the Lifeline program.[1] TerraCom provides prepaid local, intrastate, and interstate telecommunications services to low-income residential customers in Oklahoma and Texas. TerraCom is a certified competitive local exchange carrier and wireline eligible telecommunications carrier (ETC).[2]

[1] Lifeline service is a retail voice telephony service that telecommunications carriers provide to qualifying low-income consumers for a reduced charge. 47 C.F.R. § 54.407(b). *See also Lifeline and Link Up Reform and Modernization*, Report and Order and Further Notice of Proposed Rulemaking, 27 FCC Rcd 6656, 6662–67, paras. 11–18 (2012) (*Lifeline Reform Order*); 47 C.F.R. §§ 54.400–54.422.

[2] Carriers providing Lifeline service are called "eligible telecommunications carriers," or ETCs, and are reimbursed by the Universal Service Fund for the subsidized amount of the voice service they provide to qualified consumers.
(continued....)

TerraCom is also a wireless ETC for Lifeline services in fourteen states, Puerto Rico, and the Virgin Islands.[3] YourTel provides wireless Lifeline telephone service as an ETC in eight states, and wireline Lifeline service in three.[4] TerraCom and YourTel have common shareholders, share key management employees,[5] and are joint owners of a third company, BrightStar Global Solutions, LLC (BrightStar),[6] but are separate corporate entities headquartered in Oklahoma and Missouri, respectively.[7]

4. Low income consumers who wish to obtain Lifeline services provided by TerraCom or YourTel are required to submit information and documents demonstrating that they have an income that is at or below 135% of the federal Poverty Guidelines, or that they participate in one or more of several state and federal government assistance programs (such as Medicaid, Supplemental Nutrition Assistance Program (SNAP), public housing assistance, and others). Applicants must submit, among other things, their name and address, date of birth, Social Security Number, and driver's license or state ID card. In addition, in order to determine income eligibility for Lifeline service, the Companies collect additional information from applicants, such as their annual statement of government benefits; the prior year's state, federal or Tribal tax return; paycheck stubs; Social Security benefit statements; Veterans Administration benefit statements; retirement or pension information; Unemployment or Workers' Compensation benefit statements; Federal or Tribal notice letters of participation in General Assistance; divorce decrees or child support awards; or other official documents establishing the applicant's income level.[8]

5. Applicants for the Companies' services submitted PI on electronic application forms and supplemented the applications with scanned images of PI-laden supporting documentation (described above) to establish proof of eligibility. The Companies collected this information through their respective websites and, through BrightStar, their commonly owned contracting company, retained CallCenters India, Inc., d/b/a Vcare Corporation (Vcare), to provide them with call center, back office support systems, hosted billing, and other services to support their Lifeline offerings.[9] Part of the "hosted"

(Continued from previous page)
47 C.F.R. § 54.407(b). *See also Lifeline Reform Order*, 27 FCC Rcd at 6662–67, paras. 11–18; 47 C.F.R. §§ 54.400–54.422.

[3] TerraCom provides wireless Lifeline service in Arkansas, Arizona, Colorado, Indiana, Iowa, Louisiana, Maryland, Minnesota, Nebraska, Nevada, Oklahoma, Texas, West Virginia, and Wisconsin.

[4] YourTel provides wireless Lifeline service in Illinois, Kansas, Maine, Missouri, Oklahoma, Pennsylvania, Rhode Island, and Washington.

[5] TerraCom's and YourTel's Chief Operating Officer (COO) is Dale Schmick.

[6] BrightStar Global Solutions, LLC is an Oklahoma limited liability company located at 1101 Territories Dr., Edmond, OK 73034. TerraCom describes BrightStar as "[redacted]." *See* Letter from Mark C. Del Bianco, Law Office of Mark C. Del Bianco, Attorney for TerraCom and YourTel, to Steven Ruckman, Esq., Assistant Attorney General, Maryland Office of the Attorney General, (June 14, 2013) (on file in EB-TCD-13-00009175) (Maryland AG Letter of Jun. 14, 2013).

[7] According to the respective 499s of TerraCom and YourTel, the Companies share the same corporate headquarters address at 401 E. Memorial, Suite 400, Oklahoma City, OK 73114. However, according to YourTel's 2013-2014 Biennial Registration Report with the Missouri Secretary of State, the company's principal place of business or corporate headquarters is 2800 E. 18th Street, Kansas City, MO 64127. *See* YourTel America, Inc. 2013-2014 Biennial Registration Report (Mar. 20, 2013), *available at* Missouri Sec. of State, Online UCC Filing, https://bsd.sos.mo.gov/BusinessEntity/BusinessEntityDetail.aspx?page=beSearch&ID=356173.

[8] *See* 47 C.F.R. § 54.410; *see also* E-mail and attachment from Matt Connolly, Manager, Regulatory Affairs, YourTel America, Inc., to Donna Cyrus, Senior Attorney Advisor, Telecommunications Consumers Division, FCC Enforcement Bureau (July 17, 2013, 17:02 EDT) (on file in EB-TCD-13-00009175) (TerraCom/YourTel LOI Response).

[9] *See* Letter of Intent From Call Centers India DBA Vcare Corporation to BrightStar Global Solutions, LLC (Jul. 10, 2012) (on file in EB-TCD-13-00009175) (Vcare Agreement). [redacted],
(continued....)

services that the Companies' purchased from Vcare included software and electronic storage on dedicated data servers to house the collected documents and applications. From September 30, 2012, through April 26, 2013, the Companies stored these electronic forms and scanned documents on Vcare's servers in [redacted].[10] The Companies stored the PI-containing documents in clear, readable text and in electronic format accessible via the Internet.

6. In early 2013, an investigative reporter working for Scripps Howard News Service (Scripps) discovered that the Companies were storing PI and documents submitted by low income Lifeline service applicants on an unprotected Internet site. Between March 24, 2013, and April 26, 2013, Scripps accessed at least 128,066[11] confidential records and documents submitted by subscribers and applicants for the Companies' services.[12] Scripps located a consumer's data file by conducting a simple Google search.[13] Once it had located a single file, Scripps shortened that file's URL and obtained access to the entire directory of applicant and subscriber data.[14] On April 26, 2013, Scripps alerted the Companies that it had accessed their servers and had retrieved the PI of subscribers and applicants stored there.[15]

7. On April 30, 2013, TerraCom and YourTel sent a "cease and desist" letter to Scripps, referring to Scripps' reporters as "hackers" who had illegally accessed "directories on Vcare's servers that contained all of the Lifeline applications processed by Vcare since April 2012."[16] According to the letter,

(Continued from previous page)
Vcare provided a variety of services purchased by the Companies [redacted] to enable their provision of Lifeline services, including, among other things, front end website and backend application flow and processing, customer account activations, support for lifeline enrollments, including processing customer applications, certain integration and gateway services, and call center services. *See* Vcare Agreement at 1–3; *see also JLee-Cease-and-Desist-Ltr*, torekeland.com, *available at* https://torekeland.com/wp-content/uploads/2013/05/JLee-Cease-and-Desist-Ltr.pdf (last visited Oct. 17, 2014).

[10] The Companies were not specific about the exact date in September 2012 when they began storing PI on Vcare's servers, so for purposes of this Notice of Apparent Liability for Forfeiture, we will attribute this date to September 30, 2012. *See* E-mail from Douglas D. Orvis II, Bingham, Counsel to TerraCom and YourTel , to Donna Cyrus, Senior Attorney Advisor, Telecommunications Consumers Division, Enforcement Bureau, FCC (Jan. 24, 2014, 15:09 EDT) (on file in EB-TCD-13-00009175) (January 24, 2014, E-mail).

[11] *See* Letter from Douglas D. Orvis II, Bingham, Counsel to TerraCom and YourTel, to Kimberly Wild, Deputy Division Chief, Telecommunications Consumers Division, FCC Enforcement Bureau, (Nov. 19, 2013) (on file in EB-TCD-13-00009175) (TerraCom/YourTel November 19, 2013, Supplemental LOI Response).

[12] The records of 343 individuals were also accessed by unknown parties during this time. *See* TerraCom/YourTel November 19, 2013, Supplemental LOI Response. Additional, undetermined access to these records may have occurred since September 2012, "when VCare [sic] became the third party verification company for TerraCom and YourTel." *See* January 24, 2014, E-mail.

[13] *Isaac Wolf Accesses Lifeline Files,* NewsNet5 Cleveland (May 19, 2013), *available at* http://www.newsnet5.com/news/local-news/special-reports/privacy-on-the-line-security-lapse-exposes-some-lifeline-phone-customers-to-id-theft-risk

(last visited September 4, 2014).

[14] *Id.*

[15] E-mail from Isaac Wolf, Scripps Howard News Service, to Dale Schmick, COO, TerraCom and YourTel (Apr. 26, 2013, 11:17 EDT) (on file in EB-TCD-13-00009175), *available at* http://media.thedenverchannel.com/documents/Scripps%20email%20requesting%20interview.pdf.

[16] Letter from Jonathan D. Lee, Principal, JD Lee Consulting, and Counsel, TerraCom, Inc. and YourTel America, Inc., to William Appleton, Senior Vice President/General Counsel, The E.W. Scripps Company, *available at* media.thedenverchannel.com/documents/Response%20from%20Jonathan%20Lee.pdf (Apr. 30, 2013) (Scripps Cease and Desist Letter) (on file in EB-TCD-13-00009175).

between March 24, 2013, and April 26, 2013, Scripps employees downloaded at least 19,000 applications for Lifeline service and 127,000 files containing eligibility/income documentation.[17]

8. On May 7, 2013, the Companies contacted the Enforcement Bureau (Bureau), about the data breach.[18] TerraCom and YourTel claimed that the Companies "were victims of a security breach resulting from unauthorized access to personal data by an investigative reporter from [Scripps]."[19] TerraCom and YourTel stated that the compromised data belonged to "applicants seeking enrollment in the Lifeline program."[20] Additionally, the evidence shows that 343 records "were viewed by unknown, and potentially unauthorized, individuals."[21]

9. Ten days after alerting the Enforcement Bureau to Scripps' access to the data, the Companies sent a letter to the FCC's Wireline Competition Bureau to explain that their service provider, Vcare, was retaining [redacted].[22]

10. On June 17, 2013, the Bureau sent a letter of inquiry (LOI) jointly to TerraCom and YourTel directing each company to provide information regarding the reported security breach, among other things.[23] The Companies provided their response on July 17, 2013.[24]

III. DISCUSSION

11. As discussed at length below, Section 222(a) imposes a duty on TerraCom and YourTel to protect the confidentiality of this information.[25] Likewise, Section 201(b) of the Act requires

---

[17] *Id.*

[18] *See* E-mail and attachments from Mark Del Bianco, Esq., Law Office of Mark C. Del Bianco, Attorney for TerraCom and YourTel, to Donna Cyrus, Senior Attorney Advisor, Telecommunications Consumers Division, FCC Enforcement Bureau (May 7, 2013, 23:32 EDT) (on file in EB-TCD-13-00009175) (May 7, 2013, E-mail).

[19] *Id.*

[20] *Id.*

[21] Isaac Wolf, *Privacy on the Line: Security lapse exposes some Lifeline phone customers to ID theft risk*, Scripps News (May 20, 2013), *available at* http://www.kjrh.com/news/local-news/investigations/privacy-on-the-line-security-lapse-exposes-some-lifeline-phone-customers-to-id-theft-risk; *see also* May 7, 2013, E-mail (the Companies stated that their investigation "revealed that the records of approximately 343 individuals were accessed one or two at a time from IP addresses whose owners we cannot confirm at this time.").

[22] *See* Letter from Jonathan D. Lee, Esq., Principal, JD Lee Consulting, Counsel for TerraCom and YourTel, to Radhika Karmarkar, Deputy Division Chief, Telecommunications Access Policy Division, FCC Wireline Competition Bureau (May 17, 2013) (on file in EB-TCD-13-00009175) (May 17, 2013, Letter).

[23] *See* Letter from Richard A. Hindman, Chief, Telecommunications Consumers Division, FCC Enforcement Bureau, to Mark C. Del Bianco, Esq., and Jonathan D. Lee, Esq., Counsel for TerraCom and YourTel (June 17, 2013) (on file in EB-TCD-13-00009175) (LOI).

[24] *See* TerraCom/YourTel LOI Response. The LOI was addressed to both Companies and required each entity to answer questions with respect to that entity's operations. The Companies filed a joint response to the Bureau's inquiries on behalf of both companies, but they indicated that TerraCom and YourTel are unaffiliated corporations. Accordingly, to the extent the answers submitted by the Companies identify a single company, we attribute that answer to the identified company; when the responses do not specify either TerraCom or YourTel individually, we attribute that answer to both Companies. Moreover, in their joint letters to the Wireline Competition Bureau and in their initial responses to the Enforcement Bureau's inquiries, the Companies referred to each other jointly and identified themselves as affiliates.

[25] 47 U.S.C. § 222(a).

TerraCom's and YourTel's practices related to such information and consumers to be "just and reasonable" and declares unlawful any practice that is unjust or unreasonable.[26]

12. As discussed more fully below, we charge TerraCom and YourTel with apparently violating (1) Section 222(a) of the Act for failing to protect the confidentiality of PI that consumers provided to demonstrate eligibility for Lifeline telecommunications services; (2) Section 201(b) of the Act by failing to employ reasonable data security practices to protect consumers' PI; (3) Section 201(b) of the Act by representing in their privacy policies that they protected customers' personal information, when in fact they did not; and (4) Section 201(b) of the Act by failing to notify all customers whose personal information could have been breached by the Companies' inadequate data security policies.

- TerraCom and YourTel apparently violated Section 222(a) of the Act for failing to protect the confidentiality of PI that consumers provided to demonstrate eligibility for Lifeline services. The Companies collected consumers' PI through the Companies' websites[27] and until April 26, 2013, stored, or their vendor stored, this PI in clear, readable text on one or more servers in [redacted] that were accessible via the Internet.
- By failing to employ reasonable data security practices to protect consumers' PI, the Companies also engaged in an unjust and unreasonable practice in apparent violation of Section 201(b) of the Act. They failed to use even the most basic and readily available technologies and security features and thus created an unreasonable risk of unauthorized access.
- TerraCom and YourTel also apparently violated Section 201(b) of the Act by representing in their privacy policies that they protected customers' personal information, when in fact they did not. The Companies' privacy policies and statements on their websites inform consumers that they have "implemented technology and security features to safeguard the privacy of your customer specific information from unauthorized access or improper use" and that they "continue to enhance its security measures as technology becomes available."[28] The evidence shows, however, that TerraCom and YourTel, in fact, collected PI through their websites and failed to employ reasonable practices to safeguard this information as they represented, expressly or by implication, in their privacy policies.
- Finally, we find that the Companies engaged in an unjust and unreasonable practice in apparent violation of Section 201(b) by failing to notify all customers whose personal information could have been breached by the Companies' inadequate data security policies. The Companies exposed over 300,000 consumers to potential data security breaches through their lax and virtually non-existent security practices. When learning that a security breach had occurred, the

[26] 47 U.S.C. § 201(b).

[27] *See* TerraCom/YourTel LOI Response at 6, stating "Vcare provides the entrance portal through which applicant order information is collected and delivered for processing and storage on Vcare owned servers." *See also JLee-Cease-and-Desist-Ltr*, torekeland.com, *available at* https://torekeland.com/wp-content/uploads/2013/05/JLee-Cease-and-Desist-Ltr.pdf (last visited Oct. 17, 2014).

[28] *See* TerraCom Privacy Policy, terracomwireless.com, https://web.archive.org/web/20110924070048/http://www.terracomwireless.com/privacy/ (archived Sept. 24, 2011) (accessed by searching for TerraCom, Inc. Privacy Policy in the Internet Archive) (on file in EB-TCD-13-00009175); YourTel Privacy Policy, yourtelwireless.com, https://web.archive.org/web/20110521001951/http://www.yourtelwireless.com/privacy/ (archived May 21, 2011) (accessed by searching for YourTel America, Inc. Privacy Policy in the Internet Archive) (on file in EB-TCD-13-00009175) (archived copies of the privacy policies of TerraCom and YourTel prior to September 2012). *See also* TerraCom Privacy Policy, www.terracomwireless.com/privacy.php (last visited Sept. 4, 2014), YourTel Privacy Policy, www.yourtelwireless.com/privacy.php (last visited Sept. 4, 2014) (current privacy policies of the Companies, respectively).

Companies failed to notify all potentially affected consumers and thereby deprived them of any opportunity to take steps to protect their PI from misappropriation by third parties.

Each of the above charges is discussed more fully below.

A. TerraCom and YourTel Apparently Violated Section 222(a) of the Communications Act By Breaching Their Statutory Duty to Protect the Privacy of Proprietary Information

13. We find that TerraCom and YourTel apparently willfully and repeatedly violated Section 222(a) of the Act. Section 222(a) imposes a duty on every telecommunications carrier "to protect the confidentiality of proprietary information of, and relating to . . . customers."[29] The Commission has made clear that section 222(a) requires carriers to "take every reasonable precaution to protect the confidentiality of proprietary or personal customer information"[30] and that it was "committing to taking resolute enforcement action to ensure that the goals of section 222 are achieved."[31] As discussed below, the information that TerraCom and YourTel collected from consumers when applying for their Lifeline services was "proprietary information of, and relating to" their customers. The evidence shows that TerraCom and YourTel failed to fulfill their duty to protect that information.

1. The Information TerraCom and YourTel Collected from Consumers was "Proprietary Information" Under Section 222(a)

14. Congress added Section 222—entitled "Privacy of Customer Information"—to the Communications Act as part of the Telecommunications Act of 1996.[32] Section 222(a) of the Communications Act imposes a duty on every telecommunications carrier to protect the confidentiality of "proprietary information" of its customers. In the context of Section 222, it is clear that Congress used the term "proprietary information" broadly to encompass all types of information that should not be exposed widely to the public, whether because that information is sensitive for economic reasons or for reasons of personal privacy. That meaning is clear from how the word "privacy" is used in the section heading and in the heading of paragraph (c)(1), which, although it refers to "customer proprietary network information," is titled "Privacy requirements for telecommunications carriers." We therefore interpret "proprietary information" in Section 222(a), as applied to customers, as clearly encompassing private information that customers have an interest in protecting from public exposure. The Commission has consistently interpreted Section 222(a) as requiring telecommunications carriers to protect sensitive private information,[33] and we affirm that view here.

15. It is also clear that the scope of "proprietary information" protected by Section 222(a) is broader than the statutorily defined term "customer proprietary network information" (CPNI). Had Congress wanted to limit the protections of subsection (a) to CPNI, it could have done so. This interpretation of Section 222(a) is consistent with other provisions of the Communications Act that use the term "proprietary information." In the context of public broadcasting, for example, the Corporation for Public Broadcasting (CPB) must maintain for public inspection certain financial information about programming grants. But Congress also recognized that "proprietary, confidential, or privileged information" should not be made public, and Congress thus expressly excluded such information from

[29] *See* 47 U.S.C. § 222(a).

[30] *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).

[31] *Id.* at 6959–60, para. 65.

[32] Telecommunications Act of 1996, Pub. L. No. 104-104, 110 Stat. 56 (1996 Act) (codified at 47 U.S.C. §§ 151 *et seq.*).

[33] *See, e.g., supra* note 30.

public disclosure.[34] Similarly, in the context of establishing rules for fair competition in the telephone equipment manufacturing market in 1996, Congress added non-discrimination rules applicable to standards-setting and certification entities that review telephone equipment for interoperability and engineering purposes. Recognizing that such entities necessarily gain access to extremely valuable trade secrets, Congress explicitly prohibited those review entities from "releasing or otherwise using any proprietary information" belonging to the manufacturer without written authorization.[35]

16. The overarching principle is that we should interpret the term "proprietary information" in the commonly understood sense of information that should not be exposed widely to the public, so when applied to information about individuals, the term must include personal data that customers expect their carriers to keep private,[36] including information a carrier may possess that is not subject to the additional restrictions afforded to carrier treatment of CPNI.[37]

17. As evidenced by the foregoing examples, the term "proprietary information" in Section 222(a) broadly encompasses such confidential information as privileged information, trade secrets, and personally identifiable information (PII). In general, PII is information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context. Additionally, while we do not formally adopt it here, we find the definition of PII used by the National Institute of Standards and Technology (NIST) to be informative. Under the definition used by NIST, PII is "(1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information."[38]

18. In the context of Lifeline service at issue here, "proprietary information" includes all documentation submitted by a consumer or collected by an ETC to determine a consumer's eligibility for Lifeline service, as well as all personally identifiable information contained therein. Specifically, information such as a consumer's (i) first and last name; (ii) home or other physical address; (iii) email address or other online contact information, such as an instant messaging screen name that reveals an individual's email address; (iv) telephone number; (v) Social Security Number, tax identification number, passport number, driver's license number, or any other government-issued identification number that is unique to an individual; (vi) account numbers, credit card numbers, and any information combined that

[34] *See* 47 U.S.C. § 396(l)(4)(C) ("The Corporation shall make available for public inspection the final report required by the Corporation on an annual basis from each recipient of funds under subsection (k)(3)(A)(iii)(III) of this section, excluding proprietary, confidential, or privileged information.").

[35] *See* 47 U.S.C. § 273(d)(2). This prohibition against unauthorized use or release of proprietary information continues "even after such [standards-setting or certification] entity ceases to be so engaged [by the equipment manufacturer]." *Id.*

[36] *See also, e.g.*, 47 U.S.C. § 272(d)(3)(C) (in the context of joint federal/state biennial audits of Bell Operating Company affiliates, requiring State commissions to "implement appropriate procedures to ensure the protection of any proprietary information submitted to it" as part of the audits); 47 U.S.C. § 274(b)(9) (in the context of rules applicable to BOCs and BOC affiliates with respect to joint ventures for the provision of electronic publishing services, requiring "reasonable safeguards to protect any proprietary information" contained in certain reports made available for public inspection).

[37] *See* 47 U.S.C. § 222(c) (defining telecommunications carriers' obligations with respect to CPNI); *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, 28 FCC Rcd 9609, 9618 ¶ 27 ("We also note that subsection (a)'s obligation to protect customer information is not limited to CPNI that the carrier has obtained or received.").

[38] *See* National Institute of Standards and Technology, *Guide to Protecting the Confidentiality of Personally Identifiable Information*, SP 800-122, *available at* http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf (last accessed Sep. 11, 2014); *see also* GAO Report 08-536, *Privacy: Alternatives Exist for Enhancing Protection of Personally Identifiable Information* (May 2008), *available at* http://www.gao.gov/new.items/d08536.pdf.

would allow access to the consumer's accounts; (vii) Uniform Resource Locator ("URL") or Internet Protocol ("IP") address or host name that identifies an individual; or (viii) any combination of the above, constitutes "proprietary information" protected by Section 222(a).

19. In recognizing the application of "proprietary information" in this way, we maintain the high expectations for protection that the Commission has previously articulated in other Lifeline orders. In a rulemaking order creating the National Lifeline Accountability Database, which now receives and processes from ETCs the same type of sensitive information about consumers that is at issue here, the Commission identified subscriber eligibility information as sensitive personal information.[39] Specifically, in the *Lifeline Reform Order* the Commission identified Lifeline program enrollment information as "particularly sensitive information" that "must be subject to the highest protections."[40] Just as the Commission recognized the sensitivity of this type of information in designing its own protections, to satisfy their duty under Section 222(a) to protect the confidentiality of customers' PI, carriers should know that they must likewise subject such information to the highest protections.

20. The information that the Companies collected falls squarely within the definition of "proprietary information" described above. A sampling of that information includes "completed Lifeline application forms that contain the names, addresses, social security numbers and telephone numbers of applicants ... [and] account numbers for government programs."[41] The "[d]ata accessed also included copies of 'Proof Documents' demonstrating each applicant's eligibility for the Lifeline program ... [which] included driver's licenses, benefits statements, benefit program cards, tax forms and other government forms."[42] Thus, we find that the eligibility information the Companies collected falls within the statutory protections afforded consumers under Section 222(a).

2. Lifeline Applicants Provided the Companies with Information that was "Relating to . . . Customers" Under Section 222(a)

21. The Lifeline eligibility information that TerraCom and YourTel collected related to the Companies' customers. The Companies argue that they collected the eligibility information merely from *applicants* seeking service and that applicants are not "customers" for which a duty arises under Section 222(a). Further, the Companies argue that a portion of these "applicants" were rejected and never became customers.[43] The essence of the Companies' argument is that a carrier's duty to protect a consumer's PI under Section 222(a) is not triggered unless and until that consumer becomes an actual subscriber of service. We disagree.

22. First, consumers applying for telecommunications services have a reasonable expectation that the carrier will protect the confidentiality of the PI they provide as part of that transaction. This is especially true in the Lifeline context where carriers offer a subsidized service pursuant to a government program that requires collection of PI to determine eligibility. The fact that our rules require carriers to collect PI and determine eligibility for Lifeline service *before* providing the service (i.e., before the

[39] *Lifeline Reform Order*, 27 FCC Rcd at 6745, para. 207.

[40] *Id.*

[41] TerraCom/YourTel LOI Response at 3; *see also Phone Carriers Expose Low-Income Applicants to Risk of ID Theft,* thedenverchannel.com, *available at* http://www.thedenverchannel.com/news/privacy-on-the-line/phone-carriers-expose-low-income-applicants-to-risk-of-id-theft (last visited Oct. 17, 2014).

[42] *Id.*

[43] *See* TerraCom/YourTel November 5, 2013, Clarification Response at 2, stating, "The Company also objects to the categorization of these persons as "customers", as it assumes, without proper foundation, that the applicants identified in the databases of the Company are all enrolled customers. That is not correct." According to the evidence, the Companies believed that only 20,150 of approximately 151,000 records downloaded by Scripps belonged to applicants and not customers. *See* E-mail from Salil Gupta, Vcare, to Dale Schmick, COO, TerraCom/YourTel (May 8, 2013, 16:18 EDT) (on file in EB-TCD-13-00009175).

consumer becomes a subscriber) does not change the consumers' expectations or the carrier's duty under Section 222(a) to protect consumers' PI.[44] This is no different, for example, than a consumer entering a wireless carrier's retail store and applying for service. As part of the transaction, the clerk typically asks the consumer to divulge his or her name, address, and credit card information, among other things. In handing over that information, the consumer places trust and confidence in the carrier to protect his or her privacy and the customer relationship is established for purposes of Section 222(a).[45]

23. Moreover, the Commission has recognized the applicability of privacy laws, including Section 222(a), at the pre-subscriber stage of a transaction. In the *Lifeline Reform Order* the Commission discussed carriers' responsibility to determine eligibility and recognized that to satisfy this obligation, they would collect information about prospective customers that is particularly sensitive at the application stage.[46] The Commission drew no distinction between an applicant for service and a subscriber. Thus, we find that the carrier/customer relationship commences when a consumer applies for service. The duty to protect the confidentiality of PI is triggered when the carrier accepts confidential private information as part of that transaction.

24. Additionally, the Companies themselves recognize that applicants for their services are "customers." Both TerraCom and YourTel invite consumers to apply for Lifeline service on their websites, and draw absolutely no distinctions between "applicants" and "customers." Both TerraCom and YourTel require applicants to complete a "Lifeline Certification Form" and to provide information sufficient to prove eligibility. The Companies' Lifeline Certification Form identifies persons completing the form (i.e., persons applying for Lifeline service) as "customers." In fact, the Companies use "customer" on every applicable section of the form, including the certification and signature block ("Customer Signature"). TerraCom and YourTel cannot have it both ways. They cannot invite consumers to apply for Lifeline services and upload PI on their respective websites, ignoring any distinctions on one hand, and then on the other hand, argue that the Lifeline eligibility documents these very same consumers were invited to upload are not PI and should not be protected because the applicants are not customers.

25. Further, in their privacy policies the Companies draw no distinction between "applicants" and "customers." By way of example, the Companies invite each applicant for Lifeline service to upload his or her eligibility documents directly from their privacy policy page on their websites. The Companies' privacy policies assure those persons submitting "[c]ustomer specific information" through their website that they will protect that information and, in fact, inform such applicants that "[b]y providing us with your information, you acknowledge that you have read this privacy policy, understand it, agree to its terms and consent to the transfer of such information outside your resident jurisdiction."[47] Based on the forgoing, any consumer acting reasonably under the circumstances, when confronted with the paperwork and privacy policy provided by each company for completing an application, would certainly understand himself or herself to be a customer of TerraCom or YourTel at the application stage prior to becoming a subscriber.[48] Indeed, under the Companies' logic, a mere "applicant" would be consenting to a privacy policy that does not even apply to a person with that status; in other words, if

[44] In this regard, Section 54.410 of our rules bars the Companies from activating a consumer's Lifeline service "unless and until it has . . . [c]onfirmed that the consumer is a qualifying low-income consumer . . . [and] [c]ompleted the eligibility determination . . . ." 47 C.F.R. § 54.410(a)(1)–(2).

[45] Black's Law Dictionary defines "customer" to include "[a] buyer, purchaser, consumer or patron," while Random House defines "customer" as "a patron, buyer, or shopper." Customer, Black's Law Dictionary (5th ed. 1979); customer, The Random House College Dictionary (1973).

[46] *See supra* paras. 14–20. *See also Lifeline and Link Up Reform and Modernization,* Notice of Proposed Rulemaking, 26 FCC Rcd 2770 para. 57, n.97 (2011).

[47] *See supra* note 28.

[48] *See* Appendix, examples of the Lifeline Certification Form used by each Company.

applicants are not customers, there would be no point in asking such persons to agree to something that is irrelevant to them.

26. Third, for the reasons discussed above and to give effect to the purpose of Section 222(a), we interpret "customer" to include both an applicant for service and a subscriber of the service.[49] Sections 222(a), (b), and (c) protect three types or categories of confidential information: (1) subsection (a) protects "proprietary information of, and relating to, other telecommunication carriers, equipment manufacturers, and customers, including telecommunications carriers reselling telecommunications services provided by a telecommunications carrier;"[50] (2) subsection (b) protects proprietary information that a carrier receives or obtains "from another carrier" (i.e., carrier information);[51] and (3) subsection (c) protects "customer proprietary network information" or CPNI.[52] Section 222(a) is the broadest of the three subsections and encompasses the other two.[53] While both subsections (a) and (c) use the term "customer," we read them flexibly to give effect to the information each subsection seeks to protect.[54]

27. In this regard, subsection (c) protects customers' CPNI and subsection (a) imposes a duty on carriers to protect customers' PI. The statute defines CPNI as "information that relates 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 is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and . . . information contained in the bills pertaining to . . . service received by a customer of a carrier."[55] The statute's use of the term "customer" in this context is integrally tied to the service purchased by a consumer. Thus, consistent with the CPNI definition, our rules define "customer" as "a person or entity to which the telecommunications carrier is currently providing service."[56] Subsection (a)'s protections, however, are broader than CPNI and impose a duty on carriers to protect PI that a carrier obtains both at the application stage when a consumer provides the carrier with such information and reasonably relies on the carrier to protect his or her PI, as

[49] In addition, the term "customer" includes both current and former applicants and subscribers.

[50] 47 U.S.C. § 222(a).

[51] 47 U.S.C. § 222(b).

[52] 47 U.S.C. § 222(c).

[53] Both subsections (a) and (b) protect the confidentiality of carrier information. *Compare* 47 U.S.C. § 222(a) *with* 47 U.S.C. § 222(b) (subsection (a) protects "other telecommunication carriers" and includes within the term "customer" carriers that resell telecommunications services). Similarly, both subsections (a) and (c) protect "customer" information—with subsection (c) limited in scope to protecting CPNI, specifically. *Compare* 47 U.S.C. § 222(a) *with* 47 U.S.C. § 222(c) (subsection (a) protects "proprietary information of . . . customers" and subsection (c) protects "customer proprietary network information").

[54] Our interpretation of "customer" in this way is consistent with established principles of statutory construction. *See, e.g., Sacramento Nav. Co. v. Salz*, 273 U.S. 326, 330 (1927) (". . . . words are . . . to be taken in the sense which will best manifest the legislative intent"). In this case, the Companies' argument that "customer" does not include applicants seeking to become subscribers of the Companies' services is an overly mechanical reading of the statute that would defeat the intent of Congress to protect consumers' personal information from public exposure. *See Lawson v. Suwannee Fruit & Steamship Co.*, 336 U.S. 198, 201 (1949) (proper to give construction to avoid overly narrow reading of statutory terms, even defined terms, that would lead to results Congress did not intend). Moreover, identical words used in different parts of the statute, or even within the same part of a statute, may be read flexibly in order to best reflect Congressional intent. *See Environmental Defense v. Duke Energy Corp.*, 549 U.S. 561, 574 (2007) (*Environmental Defense*) ("We . . . understand that most words have different shades of meaning and consequently may be variously construed, not only when they occur in different statutes, but when used more than once in the same statute or even in the same section.") (internal citations omitted).

[55] 47 U.S.C. § 222(c).

[56] 47 C.F.R. § 64.2003(f).

well as after the consumer becomes a subscriber.[57] Thus, our inclusion of applicants in the definition of customer in the context of Section 222(a) gives effect to the broader duty and privacy protections.

28. We therefore find that a plain and practical reading of the protections afforded to consumers' PI under Section 222(a) requires us to interpret the statute's reference to "customer" to include applicants as well as subscribers of a telecommunications service. Having found that Section 222(a) applies, we conclude that TerraCom and YourTel had a duty to protect the confidentiality of the PI given to them by consumers.

3. TerraCom and YourTel Apparently Breached Their Duty Under Section 222(a) to Protect Lifeline Data Belonging to Their Customers

29. The evidence shows that the Companies' security measures lacked even the most basic features to protect consumers' PI. According to Scripps and Sensei Enterprises, Inc., a company hired by the Companies to investigate the breach, the PI hosted by Vcare on its server was widely available on public websites online through a simple Google search.[58] The Enforcement Bureau independently confirmed that search engines had, in fact, not only found TerraCom's applications containing PI but downloaded and archived at least two such applications and posted them openly on the Internet. The applications remained available to anyone using the Internet as late as June 30, 2014.[59] The Companies knew or should have known that the use of random URLs without more (e.g., encryption) to protect applicant records provided inadequate security and left the documents vulnerable to exposure via search engines—which operate by visiting websites, indexing all or much of the content available on them, and then delivering links to the indexed results to anyone that queries the engine.[60]

30. By not employing appropriate security measures, TerraCom and YourTel exposed their customers to potentially substantial injury. The exposed PI—in particular, financial information and Social Security numbers—invites identify theft and other serious consumer harms. Further, the Companies' choice to store, or its vendor's choice to store, files containing the PI of customers in a publicly accessible folder on the Internet, without password protection or encryption, is the practical equivalent of having provided no security at all. Based upon the foregoing, we find that TerraCom and YourTel collected PI submitted by consumers and failed to provide adequate protection of the PI in apparent violation of Section 222(a) of the Act.

B. The Companies Failed to Employ Just or Reasonable Data Security Practices to Protect Consumers' Proprietary Information in Apparent Violation of Section 201(b)

31. TerraCom and YourTel's failure to protect and secure the PI of their customers also constitutes an unjust and unreasonable practice in apparent violation of Section 201(b) of the Act.

---

[57] *See Environmental Defense*, 549 U.S. at 574 (holding that identical words within a statute may take on different meanings, even when the words share a common, general definition, and stating that "each section [of the regulation] must be analyzed to determine whether the context gives the term a further meaning that would resolve the issue in dispute . . . .").

[58] *See* report from Sensei Enterprises, Inc., to Andy Roth, Dentons, Counsel for TerraCom and YourTel (December 13, 2013) (on file in EB-TCD-13-00009175) (Sensei Forensic Report); *see also infra* note 67.

[59] Bureau Staff contacted the site and requested removal of the archived website pages, and notified counsel for TerraCom when the website agreed to do so. *See* Email from Kristi Thompson, Deputy Division Chief, Telecommunications Consumers Division, FCC Enforcement Bureau, to Douglas D. Orvis II, Bingham, Counsel to TerraCom and YourTel (Jul. 1, 2014, 16:06 EDT) (on file in EB-TCD-13-00009175).

[60] *See* E-mail from Michael C. Maschke, Chief Information Officer, Sensei Enterprises, Inc., to Dale Schmick, COO, TerraCom and YourTel (May 14, 2013, 13:31 EDT) (on file in EB-TCD-13-00009175); *see also Crawling & Indexing*, Google, *available at* http://www.google.com/insidesearch/howsearchworks/crawling-indexing.html (last visited Oct. 17, 2014).

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 [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."[61]

32. We find the Companies' data security practices unjust and unreasonable for at least two reasons. First, the Companies failed to employ even the most basic and readily available technologies and security features for protecting consumers' PI. As discussed above, consumers' PI was stored on servers that were accessible over the public Internet. The Companies stored, or their vendor stored, this information in clear, readable text on one or more servers in [redacted] that were accessible to anyone using a simple search technique. The data was not password protected or encrypted;[62] in fact, the Companies' agreement with its vendor Vcare [redacted].[63] As we said in the context of protecting CPNI—a subset of "proprietary information" —"carriers' existing statutory obligations to protect their customers' CPNI include a requirement that carriers take reasonable steps, which may include encryption, to protect their CPNI databases from hackers and other unauthorized attempts by third parties to access CPNI."[64] We do not hold here that encrypting without more would satisfy a carrier's duty under Section 222(a) or render a carrier's data security practices just and reasonable under Section 201(b); however, given the state of the technology, we believe the lack of encryption clearly evidences the unjust and unreasonable nature of the Companies' data security practices.

33. Secondly, the Companies' data security practices created an unreasonable risk of unauthorized access. As discussed above, the Companies used random URLs to protect their customers' PI. Further, the Companies' URL naming convention for one of the folders containing PI that was stored on Vcare's server also exposed the names of the applicants or customers directly in the URL, further demonstrating the lack of security of the records.[65] In relevant part, the Sensei Forensic Report states:

[redacted].

***

[redacted]

[61] 47 U.S.C. § 201(b).

[62] *See* TerraCom/YourTel LOI Response at 3; *see also Investigative Journalists Threatened with Felony for Exposing Security Flaw*, rt.com, *available at* http://rt.com/usa/hack-terracom-security-scripps-596/ (last visited Oct. 17, 2014).

[63] *See* Maryland AG Letter of Jun. 14, 2013, at 2 (stating that the parties [redacted].

[64] *See Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, 22 FCC Rcd 6927 at 6946.

[65] The single act of placing a consumer's name in a URL may, under certain circumstances, be a breach of a carrier's duty under Section 222(a) of the Act, but when the name is linked to other proprietary information belonging to the named person (as is the case here), it is *clearly* a failure to "protect" that information and, therefore, a violation.

[redacted].[66]

In other words, the companies used URLs that contained the names of Lifeline applicants in plain text. This made it exceptionally easy to locate the confidential files to which the URLs pointed by conducting a simple Google search for names.[67]

34. The evidence shows that the Companies' data security practice of using these naming conventions was wholly insufficient to protect consumers' PI. In fact, the evidence shows that as a result of the Companies' practices, between March 24, 2013 and April 26, 2013,[68] Scripps accessed and downloaded approximately 128,066 proprietary records.[69] Further, after the breach, the Companies hired a digital forensics consultant (Sensei) to investigate the breach. Sensei traced some of the [redacted] Additionally, the evidence shows that a number of the IP addresses that accessed this data were from foreign countries, including Russia, China, Ukraine, Norway, Poland, and Slovenia.[71] Sensei reported that at least [redacted], all from [redacted], and described this as "[redacted]." These countries are often identified as hot spots for identity theft.[73]

35. In light of the Companies' practices related to their lack or near lack of any data security and the magnitude or potential for harm when consumer's PI is accessed (e.g., identify theft), we find the Companies' data security practices unjust and unreasonable in apparent violation of Section 201(b) of the Act.[74]

---

[66] *See* Sensei Forensic Report.

[67] *See Isaac Wolf accesses Lifeline files*, Naples Daily News, May 19, 2013, http://www.naplesnews.com/videos/detail/isaac-wolf-accesses-files-online-lifeline/ (last visited Jun. 26, 2014) (video of Scripps reporter Isaac Wolf demonstrating how to access TerraCom Lifeline application materials via Google searches).

[68] The Companies reported that the security breach occurred between March 24, 2013 and April 26, 2013. It is now apparent, however, that the Companies' problem of inadequate security extends well beyond these dates, to September 2012 when Vcare became the Companies' third party data processor and began storing the applicant files in publicly accessible folders. *See* January, 24, 2014, E-mail. Thus, for at least seven months, the personal information contained in the Lifeline enrollment applications and proof documents were accessible by search engines.

[69] In addition to this estimate of 128,066 provided by the Companies, the Sensei Forensic Report reports that a total of [redacted] were made by [redacted]. Scripps also reports that figure as high as 170,000. *See* Ellen Weiss, *Scripps Investigation into Security Risks Draws Scrutiny*, Scripps Howard News Service (May 15, 2013), *available at* http://www.abcactionnews.com/news/local-news/i-team-investigates/kjrh_scripps-investigation-into-security-risks-draws-scrutiny1368649588977.

[70] E-mail from Michael Maschke, Chief Information Officer, Sensei, to Dale Schmick, YourTel (May 14, 2013).

[71] TerraCom/YourTel LOI Response, Ex. 1.

[72] Sensei Forensic Report at 3.

[73] *See, e.g.*, Erik Olsen, *Losing Face: Identity Thieves Steal More Than Money*, ABC News, *available at* erikolsen.com/writing/ABC_articles/ABCNEWS_com_ID_theft.htm (last visited Sept. 4, 2014) (identifying Eastern Europe and Southeast Asia as hotspots for identity theft, because "the level of education and technical sophistication is high, and [] tracking down and prosecuting criminals can be very tricky.").

[74] While we find that the Companies apparently violated Section 201(b) in this section, because this is the first case in which we make such a finding, we decline to exercise our discretion to propose a forfeiture for such violation at this time. However, we caution other carriers that the Commission is committed to aggressive enforcement of unlawful practices related to cyber security and data protection.

C. TerraCom and YourTel Engaged in Deceptive Practices by Misrepresenting Their Security Measures to Consumers in Apparent Violation of Section 201(b) of the Act

36. Since approximately September 30, 2012, TerraCom and YourTel have disseminated privacy policies and statements on their respective websites that represent expressly or imply that they employ reasonable security measures to protect the private information of customers signing up for service on their websites. The Companies also represent that they continually update these measures to incorporate the latest technologies as they became available. For example, TerraCom made the following representation to consumers via its privacy policy at the time that it was storing PI on unsecured Internet servers in [redacted] and [redacted]:

> TerraCom Wireless has implemented technology and security features to safeguard the privacy of your customer specific information from unauthorized access or improper use and will continue to enhance its security measures as technology becomes available. Unfortunately, there is no such thing as foolproof security on the internet, and therefore, TerraCom Wireless makes no guaranties with regard to the sufficiency of our security measures.[75]

YourTel had identical language on its website.[76]

37. As discussed above, the evidence proves that no such safeguards were in place for prospective customers' Lifeline applications.[77] The Companies, in fact, employed virtually no technology or security features for this information—other than what the Companies assert were complicated URLs and passwords when their own employees sought to access the data through a dedicated portal.[78] Further, the Companies did not implement or otherwise "enhance" (as promised in their privacy policies) security measures and technologies until they were informed of a data security breach.[79] The Companies informed the Enforcement Bureau that, sometime after April 26, 2013, they instructed Vcare to: (i) use a "[redacted]"; (ii) restrict "[redacted]"; (iii) assign "[redacted]"; (iv) use a "[redacted]"; and (v) [redacted].[80]

38. Thus, we find the Companies' representations in their privacy policies were false, deceptive, and misleading to consumers who gave TerraCom and YourTel personal and private information as part of their application for the Companies' Lifeline service. We also find the Companies' disclaimers, when read in context (i.e., immediately following clear and unambiguous language representing that the Companies had implemented the necessary security features to protect private information), wholly ineffective and misleading as well.[81] The Commission has previously found that

---

[75] *See* archived and current TerraCom privacy policies, *supra* note 28.

[76] *Id.*

[77] *See supra* para. 29.

[78] The Companies claim that [redacted]" TerraCom/YourTel LOI Response at 7.

[79] *See* attachment to May 7, 2013, E-mail, Factual Submission for TCD Staff.

[80] TerraCom/YourTel LOI Response at 6–7 (identifying the security measures currently in place, and those in place at the time Scripps accessed customer proprietary information).

[81] *See STi Telecom Inc.*, Notice of Apparent Liability for Forfeiture, 26 FCC Rcd 12808, 12812 para. 10 (2011) (disclosures must be in clear and unambiguous language to ensure that they are effective.). *See also Joint FCC/FTC*

(continued....)

deceptive practices are unjust and unreasonable practices that violate Section 201(b) of the Act.[82] Accordingly, we find TerraCom's and YourTel's practices unjust and unreasonable in apparent violation of Section 201(b).[83]

D. TerraCom and YourTel Engaged in Unjust and Unreasonable Practices by Failing to Notify all Consumers Affected by the Security Breach in Apparent Violation of Section 201(b) of the Act

39. The Companies initially told the Commission that all of the subscribers or potential subscribers whose personal information had been exposed were notified of the security breach. The evidence, however, shows that TerraCom and YourTel only notified 35,129 of the over 300,000 persons whose data was exposed.[84] The Companies state that these notices were provided based on the "state-specific notification requirements for the state of residence of the affected applicant."[85] We find the Companies' notification of anything less than all potentially affected consumers unjust and unreasonable, in violation of Section 201(b) of the Act. We find the Companies' failure to notify all affected consumers of the breach unjust and unreasonable because it left consumers ignorant about the risks of identity theft problems that may occur due in whole or part to the breach—a problem made even more troubling in light of the Companies' admission that they do not know the extent or breadth of the breach.

40. The Companies' practices of limited notification when a data security breach occurs—exposing PI to potential harms such as identify theft—were unjust and unreasonable. TerraCom and YourTel stored the PI of approximately 305,000 customers in an unsecure manner, open to easy access by third parties.[86] The Companies admit that a data breach occurred.[87] The Companies' best guess of the extent of records containing PI accessed by unauthorized third-parties is 128,066 records. The

(Continued from previous page)

Policy Statement for the Advertising of Dial-Around and Other Long-Distance Services to Consumers, Policy Statement, 15 FCC Rcd 8654, 8655 (2000) (*Joint FCC/FTC Policy Statement*), stating that "Legalistic disclaimers too complex for consumers to understand may not cure otherwise deceptive messages or practices"; *id.* at 8663 (noting that prominence, proximity, and placement of disclosure in comparison to advertising representation affect effectiveness of disclosure).

[82] *See STi Telecom Inc.*, 26 FCC Rcd 12808; *Locus Telecommunications, Inc.*, Notice of Apparent Liability for Forfeiture, 26 FCC Rcd 12818 (2011)

[83] The FCC has indicated that a marketing act or practice by a carrier that would constitute an unfair or deceptive act or practice under the FTC Act likewise constitutes an unjust and unreasonable act under Section 201(b) of the Communications Act. *See* Joint FCC/FTC Policy Statement, 15 FCC Rcd at 8655; *Business Discount Plan, Inc.*, Order of Forfeiture, 15 FCC Rcd 14461 at 14468-69 paras. 15-16 (2000) (finding that "deceptive telemarketing practices constitute 'unjust and unreasonable' practices within the meaning of section 201(b)"), *recon. denied in relevant part*, Order on Reconsideration, 15 FCC Rcd 24396 at 24399, para. 8 (2000) (finding that section 201(b) grants the Commission "a more general authority to address such practices as they might arise in a changing telecommunications marketplace"); *Locus Telecommunications, Inc.*, 26 FCC Rcd at 12820, para. 7. The same principle applies here. *See, e.g., Eli Lilli & Co.*, 133 F.T.C. 763, 767 (2002) (alleging that a failure to maintain appropriate security measures was an unfair or deceptive act or practice).

[84] January 24, 2014, E-mail. In addition, the Companies posted a notice about the breach on their websites between May 2013 and November 2013. *Id.*

[85] *Id.*

[86] *See id.*; *see also infra* note 108.

[87] May 7, 2013, E-mail.

Companies admit, however, that they do not know how many records were accessed between September 2012 and April 2013—the 128,066 number is just an estimate.[88]

41. Moreover, the Companies' estimate has been an evolving story. The Companies initially told Staff in May 2013, and reiterated in June 2013, that "343 individuals had their records accessed."[89] By November 2013 the Companies "best estimate" was up to 128,066.[90] Sensei identified [redacted] as having [redacted], and that overall Sensei was not able to determine "[redacted]" [redacted], the Sensei Forensic Report further identified at least [redacted], as well as [redacted]." In addition, the evidence shows that there are IP addresses accessing the Vcare server from China, the Ukraine, Poland, Russia, and Norway, among others.[93] The Companies speculate that these and other IP addresses cannot be confirmed because they could be accessed by their employees or other authorized personnel using home computers and other devices outside the office.[94] We do not find the Companies' explanations credible. The evidence overwhelmingly shows that the Companies simply do not know how many records containing customer PI were accessed by unauthorized third parties. In fact, because web crawlers were able to access the PI stored on Vcare's servers, it is highly unlikely that the Companies will ever have a full understanding of how many files were accessed.

42. During the investigation, Staff found two TerraCom customer applications that a web crawler had retrieved, archived, and made publically available online.[95] While Staff contacted the web service and requested that these applications be taken down, Staff did not undertake a comprehensive search of other web-crawler sites. The absence of any Company notification concerning these applications and the fact that they remained exposed to anyone using the Internet as late as June 27, 2014, leads us to believe that the Companies were completely unaware of these security breaches.

43. Because all of the records stored on Vcare's servers between September 2012 and April 26, 2013 were at risk, we find that TerraCom and YourTel acted unjustly and unreasonably by failing to notify all customers whose Lifeline enrollment information was exposed to actual and potential data

[88] The Companies admit that the "number [of persons whose information was accessed] cannot be determined with absolute certainty," but that their "best estimate" is 128,066. TerraCom/YourTel November 19, 2013, Supplemental LOI Response at 2 (clarification of Question 1.a. LOI answer).

[89] May 7, 2013, E-mail; *see also* TerraCom/YourTel LOI Response at 3.

[90] TerraCom/YourTel November 19, 2013, Supplemental LOI Response at 2 (clarification of Question 1.a. LOI answer).

[91] Sensei Forensic Report at 3, 5.

[92] *Id.* at 4.

[93] TerraCom/YourTel LOI Response, Exhibit 1, IP Identify List.

[94] *See id.* at 5. The Companies state that "the personal information of a small number of subscribers or potential subscribers was accessible by unauthorized individuals via a Google search ... Given the low number and the pattern of record-by-record access, we believe that most, if not all, of these records were accessed by sales agents or other company personnel who are authorized to have access and who simply accessed the records from a home computer." *Id.*

[95] Both applications were publically available on www.archive.org, a non-profit Internet library that uses web crawlers to access and save publically available internet pages. Prior to release of this NAL, the Bureau reached out to the Internet Archive requesting that the two applications be removed. Staff notified counsel for the Companies of these additional breaches. Copies of the web pages containing these applications are on file with Staff.

security breaches (i.e., stored on Vcare's servers during this time).[96] We expect carriers to act in an abundance of caution—even to the extent of being overly inclusive—in their practices with respect to notifying consumers of security breaches. We will review a carrier's notification practices on a case-by-cases basis to determine whether it acted justly towards consumers and in a reasonable manner under the factual circumstances of a given case (i.e., taking into account the sensitivity of the consumer information, the scale and scope of a breach, the clarity and means of notification, among other things).[97]

44. Accordingly, we find that TerraCom's and YourTel's practices with respect to notifying consumers of the security breach is unjust and unreasonable in apparent violation of Section 201(b) of the Communications Act.

IV. PROPOSED FORFEITURE

45. Section 503(b)(1) of the Act states that any person who willfully or repeatedly fails to comply with any provision of the Act or any rule, regulation, or order issued by the Commission, shall be liable to the United States for a forfeiture penalty.[98] Section 503(b)(2)(B) of the Act empowers the Commission to assess a forfeiture of up to $150,000 against a common carrier for each willful or repeated violation of the Act or of any rule, regulation, or order issued by the Commission under the Act.[99] For a violation to be willful, it need not be intentional.[100] In exercising our forfeiture authority, we are required to take into account "the nature, circumstances, extent, and gravity of the violation and, with respect to the violator, the degree of culpability, any history of prior offenses, ability to pay, and such other matters as justice may require."[101] In addition, the Commission has established forfeiture guidelines, which set forth base penalties for certain violations and identify criteria that we consider in exercising our discretion in determining the penalties to apply in any given case.[102] Pursuant to the guidelines, we may adjust a forfeiture upward for violations that are egregious, intentional, or repeated, or that cause substantial harm or generate substantial economic gain for the violator.[103]

46. In determining the proper forfeiture in this case, we are guided by the principle that the protection of consumer PI is a fundamental obligation of all telecommunications carriers. Consumers are increasingly concerned about their privacy and the security of the sensitive, personal data that they must entrust to service providers of all stripes. Given the increasing concern about the security of personal data, we must take aggressive, substantial steps to ensure that carriers implement necessary and adequate

[96] As of the release date of this NAL, the Company has provided the Commission of no updates that would show that it has completed notifying each such consumer.

[97] Because this is the first time we declare a carrier's practices related to its failure to adequately notify consumers in connection with a security breach unjust and unreasonable in apparent violation of Section 201(b), we do not propose to assess a forfeiture for the apparent violations here. However, through our action today, carriers are now on notice that in the future we fully intend to assess forfeitures for such violations, taking into account the factors identified above.

[98] 47 U.S.C. § 503(b)(1)(B); *see also* 47 C.F.R. § 1.80(a)(2).

[99] The maximum forfeiture for a continuing violation by a common carrier at the time the violations took place was $1,500,000. *See Amendment of Section 1.80(b) of the Commission's Rules, Adjustment of Forfeiture Maxima to Reflect Inflation,* Order, 23 FCC Rcd 9845 (2008). In 2013, the maximum forfeiture amount was increased to $1,575,000. *See Amendment Of Section 1.80(B) Of The Commission's Rules, Adjustment of Civil Monetary Penalties to Reflect Inflation,* Order, DA 13-1615, 78 FR 49371 (Rel. Aug. 1, 2013).

[100] *Southern California Broadcasting Co.*, Memorandum Opinion and Order, 6 FCC Rcd 4387, 4388, para. 5 (1991).

[101] *See* 47 U.S.C. § 503(b)(2)(E); *see also The Commission's Forfeiture Policy Statement and Amendment of Section 1.80 of the Commission's Rules*, Report and Order, 12 FCC Rcd 17087, 17100–01, para. 27 (1997) (*Forfeiture Policy Statement*).

[102] 47 C.F.R. § 1.80(b)(8), Note to paragraph (b)(8).

[103] *Id.*

measures to protect consumers' PI. In this case, the evidence shows that TerraCom and YourTel have not taken those obligations seriously. For the reasons articulated below, we propose a total forfeiture of $10,000,000 for the apparent violations in this case.

A. Section 222(a) Violations

1. Base Forfeiture for Section 222(a) Violations

47. Neither the Commission's forfeiture guidelines nor its case law establishes a base forfeiture for violations of Section 222(a). Thus, we look to the base forfeitures established or issued in analogous cases for guidance.

48. In 2011 and 2012, the Bureau issued Forfeiture Orders for failure to timely file the annual CPNI compliance certifications required by Section 64.2009(e) of the Commission's rules (CPNI Cases).[104] Similar to this case, the driving purpose behind the Commission's actions in the CPNI Cases was enforcing the protections that Congress established in Section 222(c) for consumers' proprietary information. In the CPNI Cases, the base forfeiture was between $20,000 and $29,000 for failure to file or failure to respond to a Bureau order to file certain information regarding the carriers' CPNI filings. Alternatively, the Commission has established a $40,000 base forfeiture amount for violations of Section 201(b)'s prohibition against unjust and unreasonable carrier practices in the context of deceptive marketing to consumers.[105]

49. We find that the Companies' actions were much more egregious than the actions of the carriers in the CPNI cases; likewise, the potential harm that flowed from the Companies' failure to secure the confidential personal information of consumers from unauthorized access was significantly greater than the harm posed by a carrier's failure to file CPNI certifications in a timely manner. As discussed below, hundreds of thousands of individuals were placed at risk of exposure of very sensitive personal information, including information about their income, their eligibility for and participation in federal assistance programs, their family members, and more. This exposure could, among other potential harms, put those individuals at risk of identity theft. The affected consumers face years of hassle and significant expense of credit monitoring to prevent permanent financial harm. Similarly, while the Commission's deceptive marketing cases are broadly analogous to this case, the potential harms to individuals whose personal and financial information is exposed to the public vastly outstrip the harms typically suffered by consumers who fall prey to misleading advertising messages.

2. Number of Violations

50. As discussed above, the Companies state that from September 2012 until late April 2013, the Companies stored personal data records belonging to approximately 305,065 customers and applicants on unsecured servers.[106] The Companies stated that they do not know the total number of related

[104] *See, e.g., Nationwide Telecom, Inc.*, Order of Forfeiture, 26 FCC Rcd 2440 (2011); *Diamond Phone, Inc.*, Order of Forfeiture, 26 FCC Rcd 2451 (2011); *USA Teleport, Inc.*, Order of Forfeiture, 26 FCC Rcd 2456 (2011); *Jahan Telecommunication, LLC*, Order of Forfeiture, 27 FCC Rcd 6230 (2012); *88 Telecom Corporation*, Order of Forfeiture, 26 FCC Rcd 7913 (2011); *DigitGlobal Communications, Inc.*, Order of Forfeiture, 26 FCC Rcd 8400 (2011).

[105] *See Business Discount Plan, Inc.*, 15 FCC Rcd 14461 at14471–72; *NOS Communications, Inc. and Affinity Network Corporation*, Notice of Apparent Liability for Forfeiture, 16 FCC Rcd 8133 at 8141–42 (2001)(NOS); *Locus Telecommunications, Inc.*, Notice of Apparent Liability for Forfeiture, 26 FCC Rcd 12818 at 12820–23 (2011); *Simple Network, Inc.*, Notice of Apparent Liability for Forfeiture, 26 FCC Rcd 16669 at 16675 (2011); *STI Telecom Inc.* (Formerly Epana Networks, Inc.), Notice of Apparent Liability for Forfeiture, 26 FCC Rcd 12808 at 12810–15 (2011); *Touch-Tel USA LLC*, Notice of Apparent Liability for Forfeiture, 26 FCC Rcd 12836 at 12842–43 (2011); *Lyca Tel, LLC*, Notice of Apparent Liability for Forfeiture, 26 FCC Rcd 12827 at 12832–34 (2011); *NobelTel LLC*, Notice of Apparent Liability for Forfeiture, 27 FCC Rcd 11760 at 11765–68 (2012).

[106] *See* January 24, 2014, E-mail.

document files stored on the servers during that period.[107] Although it is likely that some customers submitted personal information on multiple documents—for example, a basic document containing name, address, and Social Security number paired with income verification documents such as SNAP benefits or federal public housing assistance benefits statements—we will assume for the purposes of calculating the forfeiture that each of the 305,065 customers and applicants had just one document stored on the unsecured servers.[108] Each document containing PI that the Companies failed to protect constitutes a separate violation for which a forfeiture may be assessed.[109] In addition, the failure by TerraCom and YourTel to protect the PI of customers constituted a continuing violation that continued for each day during the period within the statute of limitations of this case.[110] Each unprotected document constitutes a continuing violation that occurred on each of the 81 days that elapsed between February 4, 2013, and the date that the Companies remedied the failure on April 26, 2013.

3. Calculation of Proposed Forfeiture

51. Pursuant to the guidance of Section 1.80 of the FCC's rules, we look to a number of factors when we calculate a forfeiture. In this case, the Companies' apparently unlawful actions took place repeatedly and affected hundreds of thousands of consumers. Moreover, the harm caused by the Companies' actions affected an already vulnerable population—low income Americans. The Companies' apparently unlawful actions were long in duration, widespread in scope, and egregious in nature.

52. As explained above, in the past the Commission has used a base forfeiture of $29,000 per violation or day of a continuing violation that the Commission applied in prior CPNI cases. A direct application of a $29,000 base forfeiture amount to 305,065 personal data records (again, conservatively estimating that each affected customer or applicant had just one record on the Companies' unprotected servers) would result in a proposed forfeiture approaching $9 billion. Weighing the facts before us and taking into account the extent and gravity of the circumstances, we believe that a proposed forfeiture of $8,500,000[111] is sufficient to protect the interests of consumers and to deter future violations of the Act.[112]

B. Section 201(b) Violations

53. The Commission's forfeiture guidelines do not establish a base forfeiture for violations of Section 201(b). However, in other cases involving violations of Section 201(b) in the deceptive marketing and cramming contexts, the Commission has established a base forfeiture of $40,000 for each

[107] *Id.* The Companies state that they "have not been provided with information detailing the number of files stored on VCare's [sic] servers during the period that some applicant information may have been potentially accessible."

[108] Representatives of the Companies recently alleged in a meeting with Bureau staff that the number of customers and applicants may be less than the 305,065 figure previously submitted into the record by the Companies because some submissions were apparently duplicates. The actual number of affected consumers does not change the forfeiture calculation in this case. *See infra* note109.

[109] *See NOS*, 16 FCC Rcd at 8141("Each rate sheet sent to consumers constitutes a separate violation of section 201(b)"); *see also supra* note99.

[110] The applicable dates of the apparent violations related to Section 222(a) of the Act within the statute of limitations in this case are February 4, 2013, to April 26, 2013.

[111] In light of the number of violations in this case, the proposed forfeiture is well within the limits established in Section 503 of the Act. We also note that even if we were to subtract the mere applicants (that is, consumers who applied for Lifeline service from the Companies but never became subscribers) from the 305,065 affected consumers, our forfeiture calculations would still support the proposed penalty for Section 222(a) violations. Moreover, we note that each record that the Companies failed to protect separately constitutes an unjust and unreasonable act or practice prohibited by Section 201(b) of the Act for which we could assess an additional penalty of $40,000 per record.

[112] *See NOS*, 16 FCC Rcd at 8141–42.

action that constitutes an unjust and unreasonable practice by a carrier.[113] As discussed above, the Companies' website privacy policies made false representations and promises to customers by assuring them that the Companies would protect the sensitive personal information customers submitted when in fact the Companies did not protect it. The Companies' website privacy policies state that by submitting customer specific information to their website, "you acknowledge that you have read this privacy policy, understand it, agree to its terms and consent to the transfer of such information outside your jurisdiction."[114] These false promises of security are clearly unjust and unreasonable and thus violated Section 201(b). Moreover, the violations occurred on a continuing basis from February 4, 2013, until April 26, 2013. Accordingly, for the continuing violation of Section 201(b) caused by the Companies' false and misleading privacy policies, we propose a forfeiture of $1,500,000. However, in light of the fact that this is the first time we declare a carrier's practices unjust and unreasonable under Section 201(b) for failures related to (i) data security and (ii) notice to consumers in connection with a security breach, combined with the fact that we are imposing $10 million in penalties for the other violations at issue here, we exercise our discretion not to assess a forfeiture here for these apparent violations. But carriers are now on notice that in the future we fully intend to assess forfeitures for such violations.[115]

V. CONCLUSION

54. Based on the facts and record before us, we have determined that TerraCom, Inc. and YourTel America, Inc. have apparently willfully and repeatedly violated Sections 222(a) and 201(b) of the Communications Act of 1934, as amended.

VI. ORDERING CLAUSES

55. Accordingly, **IT IS ORDERED**, pursuant to Section 503(b) of the Communications Act of 1934, as amended, 47 U.S.C. § 503(b), and Section 1.80 of the Commission's rules, 47 C.F.R. § 1.80, that TerraCom, Inc., and YourTel America, Inc. are hereby **NOTIFIED** of this **APPARENT JOINT AND SEVERAL LIABILITY FOR FORFEITURE** in the amount of ten million dollars ($10,000,000), for willful and repeated violations of Sections 222(a) and 201(b) of the Communications Act of 1934, as amended, 47 U.S.C. §§ 222(a), 201(b).

56. **IT IS FURTHER ORDERED THAT**, pursuant to Section 1.80 of the Commission's rules,[116] within thirty (30) days of the release date of this Notice of Apparent Liability for Forfeiture, TerraCom, Inc. and YourTel America, Inc. **SHALL PAY** the full amount of the proposed forfeiture for which they are jointly and severally liable, or each **SHALL FILE** a written statement seeking reduction or cancellation of the proposed forfeiture.

57. *Payment Instructions.* Payment of the forfeiture must be made by check or similar instrument, wire transfer, or credit card, and must include the NAL/Account Number and FRN referenced above. TerraCom, Inc. and YourTel America, Inc. shall send electronic notification of payment to Johnny Drake at johnny.drake@fcc.gov on the date said payment is made. Regardless of the form of payment, a completed FCC Form 159 (Remittance Advice) must be submitted.[117] When completing the FCC Form 159, enter the Account Number in block number 23A (call sign/other ID) and enter the letters "FORF" in

[113] *See Business Discount Plan, Inc.*, 15 FCC Rcd 14461 at 14471–72; *NOS*, 16 FCC Rcd at 8141–42; *Locus Telecommunications, Inc.*, 26 FCC Rcd at 12820–23; *Simple Network, Inc.*, 26 FCC Rcd at 16675; *STI Telecom Inc.*, 26 FCC Rcd at 12810–15; *Touch-Tel USA LLC*, 26 FCC Rcd at 12842–43; *Lyca Tel, LLC*, 26 FCC Rcd at 12832–34; *NobelTel LLC*, 27 FCC Rcd at 11765–68.

[114] *See supra* note 28.

[115] *See supra* notes 74, 97.

[116] 47 C.F.R. § 1.80.

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

block number 24A (payment type code). Below are additional instructions the Companies should follow based on the form of payment they select:

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

58. Any request for full payment over time under an installment plan should be sent to: Chief Financial Officer—Financial Operations, Federal Communications Commission, 445 12th Street, SW, Room 1-A625, Washington, DC 20554.[118] If the Companies have questions regarding payment procedures, they should contact the Financial Operations Group Help Desk by phone, 1-877-480-3201, or by e-mail, ARINQUIRIES@fcc.gov.

59. *Response Instructions.* The response, if any, must be mailed both to the Office of the Secretary, Federal Communications Commission, 445 12th Street, SW, Washington, DC 20554, ATTN: Enforcement Bureau—Telecommunications Consumers Division, and to Richard A. Hindman, Chief, Telecommunications Consumers Division, Enforcement Bureau, Federal Communications Commission, 445 12th Street, SW, Washington, DC 20554, and must include the NAL/Acct. No. referenced in the caption.

60. If the Companies choose to file a response seeking reduction of the proposed forfeiture on the basis of mitigation of harms caused by the apparently unlawful conduct described herein, the response must include (1) specific representations and warranties describing in detail such mitigation measures, (2) a signed declaration in compliance with Section 1.16 of the Commission's rules,[119] and (3) a request for reduction in forfeiture. The Commission may consider reducing the forfeiture if the Companies demonstrate that they have done or have entered into binding contracts to do one or more of the following:

- notified all affected consumers that their proprietary information was compromised;
- provided free credit monitoring services to all affected consumers (and will continue to provide such service for ten years in the future);
- assessed the scope of financial, reputational, or other harm that resulted from the apparently unlawful conduct and has made appropriate restitution to all affected consumers (including, but not limited to, providing restitution to consumers whose identities may have been stolen and/or credit rating harmed after the apparently unlawful conduct took place);

[118] *See* 47 C.F.R. § 1.1914.

[119] *See* 47 C.F.R. § 1.16.

- provided a hotline and website where affected consumers may contact the Companies to report instances of identity theft or other harm in order to receive credit monitoring and other assistance from the Companies;
- appointed a Chief Privacy Officer as a permanent management position to oversee notification to affected consumers and administration of credit monitoring and other remediation measures;
- conducted training of all employees of the Companies concerning restitution to consumers, data security, and privacy protection policies;
- adopted industry best practices for data security and handling of confidential information as established by reputable organizations such as the National Institute of Standards and Technology;
- conducted independent third-party security audits of all online systems and systems that store proprietary information.

The Commission may consider any or all mitigation efforts declared by the Companies when evaluating a request for reduction in forfeiture. Any such reductions in forfeiture shall be at the discretion of the Commission, and may not be calculated on a dollar-for-dollar basis.[120]

61. The Commission will not consider reducing or canceling a forfeiture in response to a claim of inability to pay unless the petitioner submits: (1) federal tax returns for the most recent three-year period; (2) financial statements prepared according to generally accepted accounting practices; or (3) some other reliable and objective documentation that accurately reflects the petitioner's current financial status. Any claim of inability to pay must specifically identify the basis for the claim by reference to the financial documentation submitted.

62. **IT IS FURTHER ORDERED** that a copy of this Notice of Apparent Liability for Forfeiture shall be sent by Certified Mail Return Receipt Requested and First Class Mail to TerraCom, Inc. and YourTel America, Inc., Attn: Douglas D. Orvis, II, Esq., Bingham McCutchen LLP, 2020 K Street, NW, Washington, D.C. 20006-1806.

FEDERAL COMMUNICATIONS COMMISSION

Marlene H. Dortch
Secretary

[120] *See* 47 U.S.C. § 503(b)(2)(E) (authorizing the Commission to determine the amount of forfeitures by taking into account such factors "as justice may require.").

STATEMENT OF
CHAIRMAN TOM WHEELER

Re: TerraCom, Inc. and YourTel America, Inc., Notice of Apparent Liability for Forfeiture, File No. EB-TCD-13-00009175

Today, the Commission is proposing a $10 million fine against two companies that failed to adequately secure the personal information of their customers. These companies have a duty under the Communications Act to protect the confidentiality of their customers' personal information. As the nation's expert agency on communications networks, the Commission cannot – and will not – stand idly by when a service provider's lax data security practices expose the personal information of hundreds of thousands of the most vulnerable Americans to identity theft and fraud.

Let's be clear about the facts: The companies in question collected sensitive information from low-income consumers to establish their eligibility for the Lifeline program. This collection is consistent with our rules, and the companies promised in their privacy policies to safeguard this information. But rather than safeguarding the information, the companies outsourced this responsibility to a vendor that collected and stored customers' Social Security numbers, names, addresses, driver's licenses, and other sensitive information on unprotected Internet servers.

In other words, the most sensitive, personal information of up to 305,000 Americans was available to anyone with an Internet connection anywhere in the world. We do not need detailed ex ante rules and regulations to know that this is simply unacceptable. Failure to take reasonable steps to secure consumer information is a clear breach of a carrier's duty to protect the confidentiality of the customer information they collect and an "unjust and unreasonable practice" – both violations of the companies' statutory obligations under the Communications Act.

Consumers entrust their most personal, confidential, and sensitive information to our communications networks and service providers every day. The Commission has a responsibility under the Communications Act to ensure that those service providers and network operators take reasonable steps to honor that public trust, and to protect consumers from harm caused by violations of the Communications Act. That is exactly what we are doing today.

STATEMENT OF
COMMISSIONER MIGNON CLYBURN

Re: TerraCom, Inc. and YourTel America, Inc., Apparent Liability for Forfeiture, File No. EB-TCD-13-00009175

The single most critical piece of one's personal information is the nine-digit number assigned to you at birth. That social security number is your first and continuous link to wages, earnings and benefits, and stays with you for eternity. Headlines reporting significant data breaches are all too common. Once a breach occurs, there is often a long road for consumers to regain control of their personal information. Thus, it is imperative that companies in possession of our proprietary data take all appropriate measures to make sure it is not compromised.

The Commission has a clear role to ensure that providers protect sensitive information. In fact, Section 222 of the Communications Act imposes a "duty" on carriers to "protect the confidentiality of proprietary information." I find this case to be particularly egregious. These companies failed to protect the proprietary information entrusted to them. I fully support this action and sincerely hope it sends a clear signal that providers must ensure that consumers' sensitive information is protected.

DISSENTING STATEMENT OF COMMISSIONER AJIT PAI

Re: TerraCom, Inc. and YourTel America, Inc., Apparent Liability for Forfeiture, File No. EB-TCD-13-00009175

A core principle of the American legal system is due process. The government cannot sanction you for violating the law unless it has told you what the law is.[1]

In the regulatory context, due process is protected, in part, through the fair warning rule. Specifically, the D.C. Circuit has stated that "[i]n the absence of notice—for example, where the regulation is not sufficiently clear to warn a party about what is expected of it—an agency may not deprive a party of property."[2] Thus, an agency cannot at once invent and enforce a legal obligation.

Yet this is precisely what has happened here. In this case, there is no pre-existing legal obligation to protect personally identifiable information (also known as PII) or notify customers of a PII data breach to enforce. The Commission has never interpreted the Communications Act to impose an enforceable duty on carriers to "employ reasonable data security practices to protect" PII.[3] The Commission has never expounded a duty that carriers notify all consumers of a data breach of PII. The Commission has never adopted rules regarding the misappropriation, breach, or unlawful disclosure of PII.[4] The Commission never identifies in the entire Notice of Apparent Liability a single rule that has been violated.[5]

Nevertheless, the Commission asserts that these companies violated novel legal interpretations and never-adopted rules. And it seeks to impose a substantial financial penalty. In so doing, the Commission runs afoul of the fair warning rule. I cannot support such "sentence first, verdict afterward" decision-making.

---

[1] *Mullane v. Central Hanover Tr. Co.*, 336 U.S. 306, 313 (1950) ("Many controversies have raged about the cryptic and abstract words of the Due Process Clause but there can be no doubt that at a minimum they require that deprivation of life, liberty or property by adjudication be preceded by notice and opportunity for hearing appropriate to the nature of the case."); *Calder v. Bull*, 3 U.S. 386, 390 (1798) (describing an *ex post facto* law as one that "that makes an action, done before the passing of the law, and which was innocent when done, criminal; and punishes such action"); *see also Bouie v. City of Columbia*, 378 U.S. 347, 350–54 (1964) ("There can be no doubt that a deprivation of the right of fair warning can result not only from vague statutory language but also from an unforeseeable and retroactive judicial expansion of narrow and precise statutory language.").

[2] *General Electric Co. v. U.S. Environmental Protection Agency*, 53 F.3d 1324, 1328 (D.C. Cir. 1995); *see also United States v. Chrysler*, 158 F.3d 1350, 1354–55 (D.C. Cir. 1998) (discussing the "well-established rule in administrative law that the application of a rule may be successfully challenged if it does not give fair warning that the allegedly violative conduct was prohibited"); *Satellite Broad. Co. v. FCC*, 824 F.2d 1, 3 (D.C. Cir.1987) ("Traditional concepts of due process incorporated into administrative law preclude an agency from penalizing a private party for violating a rule without first providing adequate notice of the substance of the rule."); *Gates & Fox Co. v. OSHRC*, 790 F.2d 154, 156 (D.C.Cir.1986) ("[T]he due process clause prevents . . . the application of a regulation that fails to give fair warning of the conduct it prohibits or requires.").

[3] *TerraCom Order* at para. 2.

[4] The closest we've come was seven years ago when we adopted protections for another type of confidential information, customer proprietary network information (CPNI). *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 (2007). Nobody thinks those rules extend to PII.

[5] None of this should be surprising given the lead role the Federal Trade Commission has taken in recent years regarding the misappropriation, breach, and unlawful disclosure of PII.

To the extent that the circumstances giving rise to today's item merited the Commission's attention, there was a better (and lawful) path forward. We could have opened a notice-and-comment rulemaking.[6] This process would have given the public an opportunity to speak. And in turn, the agency would have had a chance to formulate clear, well-considered rules—rules we then could have enforced against anyone who violated them. Instead, the Commission proposes a forfeiture today that, if actually imposed, has little chance of surviving judicial review.

One more thing. The Commission asserts that the base forfeiture for these violations is nine billion dollars—that's $9,000,000,000—which is by far the biggest in our history.[7] It strains credulity to think that Congress intended such massive potential liability for "telecommunications carriers" but not retailers or banks or insurance companies or tech companies or cable operators or any of the myriad other businesses that possess consumers' PII. Nor can I understand how such liability can be squared with the Enforcement Bureau's recent consent decrees with these companies. Under those consent decrees, the companies paid the Treasury $440,000 and $160,000 for flouting our *actual* rules and draining the Universal Service Fund by seeking Lifeline support multiple times for the same customer.

Consumer protection is a critical component of the agency's charge to promote the public interest. But any enforcement action we take in that regard must comport with the law. For the reasons stated above, I dissent.

[6] 5 U.S.C. § 553.

[7] *TerraCom Order* at para. 52. Although the FCC decides in its grace that a lower figure is "sufficient" in these particular circumstances, *id.*, it also notes that the figure could actually be billions more. *Id.* at note 111.

DISSENTING STATEMENT OF COMMISSIONER MICHAEL O'RIELLY

Re: TerraCom, Inc. and YourTel America, Inc., Apparent Liability for Forfeiture, File No.: EB-TCD-13-00009175

Companies that collect personal information about their customers have a responsibility to take reasonable measures to protect that information. Most companies take that obligation extremely seriously because it's in their best interests. So I was disturbed to learn that YourTel and TerraCom had allowed sensitive information about their universal service Lifeline subscribers to be stored in such a way that it could be accessed over the Internet through simple queries. I am also troubled that the companies did not appear to do anything to monitor the activities of their vendor to ensure that it was taking all necessary steps to protect this information. This is unacceptable for many reasons.

As unfortunate as this case may be, however, I find major flaws with the item proposed. First, I'm not convinced that the FCC has authority to act. In my previous employment, I worked extensively on privacy matters, and I am familiar with privacy laws across federal agencies. I also was there for the creation of section 222 of the Act, and it is my firm belief that it was never intended to address the security of data on the Internet. I also do not believe that section 201(b) covers this conduct. Second, even if the FCC did have authority to act, I am not persuaded that it is appropriate for the agency to proceed, in this first instance, through an enforcement action because the agency has not provided fair notice that there could be liability for such conduct. The Commission should have sought comment on these issues to determine the authority for and scope of any data security rules for common carriers. Therefore, I must respectfully dissent from this Notice of Apparent Liability for Forfeiture.

I am noticing a disturbing trend at the Commission where, in the absence of clear statutory authority, the Commission suddenly imbues an innocuous provision of the Act with tremendous significance in order to meet its policy outcome. Section 706 was one such example. Today it's section 222(a).

Section 222(a), however, cannot be interpreted in a vacuum. There is a history here, and it is worth retelling because it is relevant not only to the Commission's authority to act, but also to whether parties would have fair notice of what conduct is barred by the provision.

Those that have been following common carrier law long enough will recall that CPNI rules pre-date the Telecommunications Act of 1996. In the *Computer II*, *Computer III*, *GTE ONA*, and *BOC CPE Relief* proceedings, the Commission established rules concerning the use of CPNI in the enhanced services operations of AT&T, the BOCs, and GTE, and the CPE operations of AT&T and the BOCs. The Commission adopted these rules (along with other nonstructural safeguards) because the Commission was concerned that the carriers could use CPNI obtained from their provision of regulated services to gain an anticompetitive advantage in the unregulated CPE and enhanced services markets.[1] It also determined that the CPNI requirements were necessary to protect legitimate customer expectations of confidentiality regarding individually identifiable information.[2]

With this history in mind, and with the further understanding that one of the goals of the 1996 Act was to open local markets to competition from new telecommunications carriers, the structure and purpose of section 222 becomes evident.

Section 222(a) begins with a duty on every telecommunications carrier to protect the confidentiality of proprietary information. That is, the purpose of section 222(a) was to extend CPNI

[1] *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information,* CC Docket No. 96-115, Notice of Proposed Rulemaking, 11 FCC Rcd 12513, 12515, para. 4 (1996) (*CPNI NPRM*).

[2] *Id.*

rules to *all* telecommunications carriers, not just AT&T, the BOCs, and GTE. This was understood by the Commission at the time it was implementing the 1996 Act.[3] Then, sections 222(b) and (c) go on to codify certain restrictions to address the two concerns that led the Commission to adopt CPNI rules in the first place: to protect other carriers from anticompetitive practices; and to protect the privacy expectations of consumers.

Critically, the general duty in section 222(a) was intended to be read in conjunction with, not separate from, the specific limitations in sections 222(b) and (c). And that is how the Commission viewed the provisions.[4] Namely, section 222(a) sets forth who has the basic duty to protect the proprietary information of other telecommunications carriers, equipment manufacturers, and customers, while sections 222(b) and (c) detail when and how that duty is to be exercised. Section 222(b) requires that carriers may only use proprietary information of other carriers for the purpose of providing telecommunications and may not use it for their own marketing efforts. Section 222(c) specifies under what circumstances the proprietary information of customers (also known as CPNI) may be disclosed.

I do not see persuasive evidence that section 222(a) was intended to confer authority that was independent of the carrier information and CPNI provisions. Indeed, on multiple occasions, the Commission has made statements like "[e]very telecommunications carrier has a general duty pursuant to section 222(a) to protect the confidentiality of CPNI."[5] That is because the Commission viewed them as co-extensive.[6] In fact, it is very telling that the Commission has never before attempted to interpret 222(a) independent of CPNI. What is more, the House Conference Report on the 1996 Act notes, "[i]n

[3] *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information; Implementation of the Non-Accounting Safeguards of Sections 271 and 272 of the Communications Act of 1934, as amended*, CC Docket Nos. 96-115 and 96-149, Second Report and Order and Further Notice of Proposed Rulemaking, 13 FCC Rcd 8061, para. 194 (1998) (*CPNI Second Order and FNPRM*) ("We recognize, however, that our new CPNI scheme will impose some additional burdens on carriers, particularly carriers not previously subject to our *Computer III* CPNI requirements. We believe, however, that these requirements are not unduly burdensome. All carriers must expend some resources to protect certain information of their customers. Indeed, section 222(a) specifically imposes a protection duty; '[e]very telecommunications carrier has a duty to protect the confidentiality of proprietary information of, and relating to, other telecommunications carries, equipment manufacturers, and customers.'" (quoting 47 U.S.C. §222(a)).

[4] *Id.* paras. 204-207 (reading section 222(a) in conjunction with 222(b) and 222(c)).

[5] *See, e.g., Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, CC Docket No. 96-115, Report and Order and Further Notice of Proposed Rulemaking, 22 FCC Rcd 6927, 6931, para. 3 (2007); *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, CC Docket No. 96-115, Notice of Proposed Rulemaking, 21 FCC Rcd 1782, 1784, para. 4 (2006) (same); *CPNI Second Order and FNPRM*, 13 FCC Rcd, 8061, para. 208 ("In particular, we seek comment on whether the duty in section 222(a) upon all telecommunications carriers to protect the confidentiality of customers' CPNI, or any other provision, permits and/or requires [the Commission] to prohibit the foreign storage or access to domestic CPNI.").

[6] *See, e.g., Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, CC Docket No. 96-115, Declaratory Ruling, 28 FCC Rcd 9609, 9617, para. 24 (2013) ("Although it is certainly true that *some* of the information that carriers have collected and stored on mobile devices is not CPNI, it is equally clear that some of it is. In any event, if the information a carrier collects in the future does not meet the statutory definition, then section 222 will not apply. To reiterate, the Commission is clarifying only that information that meets the definition of CPNI is subject to section 222, just as the same information would be subject to section 222 if it were stored elsewhere on a carrier's network.") (internal citations omitted); *see id.* at 9618, para. 27 (section 222(a) helps define where but not what is covered).

general, the new section 222 strives to balance both competitive and consumer privacy interests *with respect to CPNI*."[7]

Moreover, the fact that section 222(a) uses a broader term "proprietary information" is not dispositive in this instance. Separate from my working experiences with this provision, given the three-part structure of section 222, the statute includes a term in 222(a) that encompasses both the carrier information at issue in 222(b) and the customer information at issue in 222(c).

Furthermore, I find the reliance on the section heading in this case as a source of authority just plain laughable. If the Commission can invent new authority based on the "Privacy of Customer Information" heading of section 222, I can only imagine what it could do with the heading of section 215: "Transactions Relating to Services, Equipment, *And So Forth*".[8] I suspect that those in the Commission that are asked to defend the Commission's work would also agree that section headings are of little to no value.

I do not agree that section 201(b), which dates even further back to 1934, can be read to cover data protection, and I strongly disagree with the assertion in footnote 79 that the Commission has authority to enforce unlawful practices related to cybersecurity. Moreover, if data protection falls within the ambit of 201(b), then I can only imagine what else might be a practice "in connection with" a communications service. What is the limiting principle? Perhaps recognizing that it is on shaky legal ground, the NAL at least declines to propose a forfeiture for the failure to employ just or reasonable data security practices or to notify all consumers affected by the breach.

Yet even if the Commission did have authority under section 222(a) and/or section 201(b), and I do not believe that it does, I would still have serious concerns that the Commission did not provide fair notice that the companies could be liable under those sections for this conduct. In other words, it appears the Commission is short circuiting the procedural requirements of law.

I acknowledge that the Commission has asserted in the past that it may announce new interpretations or policies in the context of an adjudication. However, "[a] fundamental principle in our legal system is that laws which regulate persons or entities must give fair notice of conduct that is forbidden or required."[9] Accordingly, "[a] conviction or punishment fails to comply with due process if the statute or regulation under which it is obtained 'fails to provide a person of ordinary intelligence fair notice of what is prohibited, or is so standardless that it authorizes or encourages seriously discriminatory enforcement.'"[10] Moreover, "[i]n the absence of notice—for example, where the regulation is not sufficiently clear to warn a party about what is expected of it—an agency may not deprive a party of property by imposing civil or criminal liability."[11]

As the FCC itself has explained, "fair notice of the obligation being imposed on a regulatee" means that "'by reviewing the regulations and other public statements issued by the agency a regulated party acting in good faith would be able to identify, with ascertainable certainty, the standards with which the agency expects parties to conform before imposing civil liability.'"[12] However, there are no regulations *at all* on section 222(a), and I am not aware of any statements that say or even hint that 222(a)

[7] H.R. REP. NO. 104-458, at 205 (1996) (CONF. REP.) (emphasis added).

[8] 47 U.S.C. § 215 (emphasis added).

[9] *F.C.C. v. Fox Television Stations, Inc.*, 132 S.Ct. 2307, 2317 (2012) (citing *Connally v. General Constr. Co.*, 269 U.S. 385, 391 (1926)).

[10] *Id.* (quoting *United States v. Williams*, 553 U.S. 285, 304 (2008)).

[11] *Trinity Broadcasting of Florida, Inc., v. FCC*, 211 F.3d 618, 628 (D.C. Cir. 2000) (quoting *General Elec. Co. v. EPA*, 53 F.3d 1324, 1328-29 (D.C. Cir. 1995)).

[12] *Infinity Broadcasting Corporation of Florida*, File No. EB-04-TP-478, Order on Review, 24 FCC Rcd 4270, 4275, para. 17 (2009) (*quoting Trinity*, 211 F.3d at 628).

and/or 201(b) covers this conduct. If there were, I would have expected them to be cited in this NAL. At most, and this is being more than generous, a very creative practitioner might have been able to imagine a scenario under which misrepresenting data security practices could fall within section 201(b). But that's it. For these reasons, and for the reasons discussed above, I do not think that the companies had fair notice and, therefore, the Commission should not propose a forfeiture. I would not be surprised to see this issue litigated at some point.

In fact, a series of agency actions (and inaction) made it *less likely* that the companies would have had fair notice. In 2007, the Commission sought comment on, among other things, requiring carriers to physically safeguard the security and confidentiality of CPNI.[13] This included questions on whether to adopt rules governing the physical transfer of CPNI among companies or to any other third party authorized to access or maintain CPNI, including a carrier's joint venture partners and independent contractors. Since the Commission included reference to this proceeding in the NAL, it certainly knows that it never acted on that part of the further notice.[14] In fact, commenters generally opposed further requirements and noted that the chief concern was access to CPNI by pretexters over the phone, not hackers seeking to gain unlawful access to carriers' CPNI databases.[15] So the issue appeared to have died. Moreover, when the Commission did act on another part of the 2007 further notice regarding data on mobile devices, it did so only after the relevant Bureaus sought further comment to refresh the record, including on whether the Commission should act by declaratory ruling, which it ultimately did. Therefore, it would have been reasonable for a regulated entity acting in good faith to believe that, at most, the Commission might act on physical safeguards, but only with respect to CPNI, and only after seeking further comment.

In sum, while I am troubled that sensitive information about Lifeline subscribers was exposed to the public, I cannot support an NAL that exceeds our authority and comes without fair notice to the companies involved. I respectfully dissent.

[13] *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, CC Docket No. 96-115, Report and Order and Further Notice of Proposed Rulemaking, 22 FCC Rcd 6927, 6961, para. 70 (2007).

[14] While the Commission has previously pursued enforcement actions despite having open rulemaking proceedings, I am concerned that open proceedings may provide companies with a false sense of security. This makes it all the more important that the Commission close open rulemaking proceedings by a date certain or as soon as it determines that it will not act on the open issues.

[15] *See, e.g.*, Comments of Verizon, CC Docket No. 96-115, WC Docket No. 04-36, at 15-17 (filed July 9, 2007); Comments of the Rural Cellular Association, CC Docket No. 96-115, WC Docket No. 04-36, at 4-5 (filed July 9, 2007); Comments of the National Cable & Telecommunications Association, CC Docket No. 96-115, WC Docket No. 04-36, at 2 (filed July 9, 2007); Comments of COMPTEL, CC Docket No. 96-115, WC Docket No. 04-36, at 2-3 (filed July 9, 2007); *but see* Consumer Coalition Comments, CC Docket No. 96-115, WC Docket No. 04-36, at 9-12 (filed July 9, 2007) (requesting that the FCC require carriers to encrypt stored CPNI and limit employee access to CPNI).