

**Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554**

In the Matter of)	
)	
Implementation of the Telecommunications Act of 1996:)	CC Docket No. 96-115
)	
Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information)	
)	
IP-Enabled Services)	WC Docket No. 04-36

**PETITION FOR RECONSIDERATION
OF CTIA – THE WIRELESS ASSOCIATION®**

Michael F. Altschul
Senior Vice President, General Counsel

Christopher Guttman-McCabe
Vice President, Regulatory Affairs

Paul W. Garnett
Assistant Vice President, Regulatory Affairs

Brian M. Josef
Director, Regulatory Affairs

CTIA – The Wireless Association®
1400 16th Street, NW, Suite 600
Washington, DC 20036
(202)-785-0081

July 9, 2007

TABLE OF CONTENTS

INTRODUCTION AND SUMMARY2

DISCUSSION.....5

I. A PRESUMPTION THAT A CARRIER HAS NOT TAKEN “REASONABLE MEASURES” IN ALL INSTANCES OF UNAUTHORIZED ACCESS TO CPNI WOULD BE CONTRARY TO LEGAL STANDARDS AND THE FCC’S ENFORCEMENT REGIME.....5

 A. The Commission’s New Enforcement Presumption Would Be Unlawful.6

 B. A Presumption Would Be Inconsistent With The Enforcement Regime In The Communications Act.11

 C. The Presumption Would Be Inconsistent With The Practice Of The Commission And Other Agencies.....14

II. THE COMMISSION SHOULD PROVIDE FURTHER GUIDANCE CONCERNING “REASONABLE MEASURES.”17

III. THE COMMISSION SHOULD MODIFY ITS DEFINITION OF “ADDRESS OF RECORD.”19

IV. THE COMMISSION SHOULD CLARIFY THAT MULTIPLE CPNI CERTIFICATIONS ARE NOT REQUIRED FOR 2007.....21

V. THE COMMISSION SHOULD CLARIFY THAT ITS RULE FOR TELEPHONE ACCESS TO CPNI ONLY APPLIES TO CUSTOMER-INITIATED CONTACT.....22

CONCLUSION.....23

**Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554**

In the Matter of)	
)	
Implementation of the Telecommunications Act of 1996:)	CC Docket No. 96-115
)	
Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information)	
)	
IP-Enabled Services)	WC Docket No. 04-36

**PETITION FOR RECONSIDERATION
OF CTIA – THE WIRELESS ASSOCIATION®**

CTIA – The Wireless Association® (“CTIA”)¹ respectfully submits this Petition for Reconsideration of the Commission’s Report and Order² in the above-captioned proceeding. While CTIA shares and supports the Commission’s efforts to safeguard customer information, this Petition is being filed to seek reconsideration of three elements of the Commission’s CPNI Order. CTIA believes that the Commission’s establishment of a presumption that carriers have failed to take “reasonable measures” in all instances of unauthorized access to CPNI would run contrary to applicable legal standards and the Commission’s enforcement regime.

¹ CTIA – The Wireless Association® is the international organization of the wireless communications industry for both wireless carriers and manufacturers. Membership in the organization covers Commercial Mobile Radio Service (“CMRS”) providers and manufacturers, including cellular, broadband PCS, ESMR, and AWS, as well as providers and manufacturers of wireless data services and products.

² Report and Order, *Telecommunications Carriers’ Use of Customer Proprietary Network Information and Other Customer Information*, 22 FCC Rcd 6927 (rel. Apr. 2, 2007) (“CPNI Order”).

INTRODUCTION AND SUMMARY

CTIA strongly supports the Commission’s decision in the CPNI Order to take additional steps to safeguard customers’ personal information from pretexters, fulfilling the congressional mandate in Section 222(a)³ of the Act to protect CPNI. The wireless industry has long shared the Commission’s goal of protecting the privacy of its customers and has taken a leadership position on this issue.⁴

CTIA agrees with the Commission that carriers should take “reasonable measures” to protect their customers’ CPNI. In particular, the Commission has required that carriers use password protections and notify the government of any breaches of CPNI.⁵ The Commission has also issued a further notice of proposed rulemaking to explore additional safeguards for protecting CPNI. These aspects of the Commission’s CPNI Order are a sensible response to the various threats from pretexters – those who make fraudulent representations to gain access to customer information – and others that would attempt to gain unauthorized access to customers’ CPNI.

There are, however, three aspects of the CPNI Order that CTIA respectfully urges the Commission to reconsider:

First, the Commission has apparently created a presumption that a carrier has not taken “reasonable measures” whenever a pretexter gains unauthorized access to CPNI. As explained further below, there is no basis to presume that a carrier has acted unreasonably or violated

³ 47 U.S.C. § 222(a).

⁴ See, e.g., CTIA Reply Comments at 3; Cingular Comments at 4-6; T-Mobile Comments at 5-7; Sprint Nextel Comments at 7-9; Verizon Wireless Comments at 3-7; see also *CPNI Order* ¶ 12.

⁵ See 47 C.F.R. § 64.2010(b)-(f) (as added by the *CPNI Order*).

Section 222(a) based on the sole fact that there has been a breach. A presumption would unfairly predetermine and lead to a legal conclusion based on a fact (the disclosure) that tells little about the appropriateness of the carrier's efforts to protect customer information. It is not reasonable to assume a carrier that has dutifully complied with the Commission's rules and has taken all other reasonable steps to protect CPNI has nonetheless *per se* acted unreasonably, particularly when there are other explanations for security breaches that may well not have been reasonably foreseeable (in the case of the increasingly sophisticated scams of data brokers) or preventable (in the case of passwords a customer may have shared with a spouse or other family members). This type of presumption would also require carriers to devote a disproportionate amount of resources to protect against any possible threat – no matter how remote. Instead, the Commission should follow its normal course in the enforcement context, maintaining the burden of persuasion on the complaining party and avoiding evidentiary presumptions. (See Part I below).

Second, the Commission should provide additional guidance concerning the contours of the “reasonable measures” standard. In particular, without having to provide for a “safe harbor,” the Commission should establish a comprehensive program for implementing the Section 222 duty to protect data, such as the program set forth in the Federal Trade Commission's Gramm Leach Bliley Act Safeguards rule. This would both require carriers to address each critical aspect of data security and give them the certainty that there is an established regulatory framework for protecting the integrity of CPNI, while providing the Commission with the flexibility to punish any “egregious” conduct. (See Part II below).

Third, the Commission should modify its new definition of “address of record” to allow carriers to provide customer service within the first 30 days following initial account

establishment. Unless modified, the new definition would forbid carriers from contacting customers within the first 30 days regarding their account. This modest change would not undermine any new protection afforded against pretexters by the Order. (See Part III below).

In addition to presenting these three issues for reconsideration, the *CPNI Order* may have also inadvertently created a requirement for carriers to prepare two “annual” certifications for calendar year 2007 – one for the period from January 1, 2007 through the *Order*’s effective date of December 8, 2007 under the old rules, and the second for the period from December 8, 2007 through December 31, 2007 under the “new” rules. The Commission should clarify that any separate certification required under the “new” rules for the brief period between December 8 and December 31, 2007, is unnecessary. Instead, the Commission should allow carriers the flexibility to include their report for that brief period in December along with their certification for calendar year 2008. (See Part IV below).

Finally, although the Commission intended that its rules for telephone access to call detail information would only apply to customer-initiated telephone contact, some of the language adopted in the final rule is slightly ambiguous as to its scope. The Commission should adopt a minor modification of its rule to eliminate this uncertainty. (See Part V below).

DISCUSSION

I. A PRESUMPTION THAT A CARRIER HAS NOT TAKEN “REASONABLE MEASURES” IN ALL INSTANCES OF UNAUTHORIZED ACCESS TO CPNI WOULD BE CONTRARY TO LEGAL STANDARDS AND THE FCC’S ENFORCEMENT REGIME.

The Commission has long established a duty on the part of carriers -- even before the enactment of Section 222 -- to protect CPNI from unauthorized disclosure.⁶ When enforcing this duty, the Commission has relied on the normal rules in enforcement matters. The complaining party carries the burden of persuasion, and there is no presumption about the reasonableness of the carrier’s conduct based on a breach.

In the CPNI Order, the Commission has for the first time apparently decided to rely on a presumption that a carrier has failed to adopt “reasonable measures” to discharge this duty (in violation of the new rule) whenever there has been a breach of CPNI by a pretexter:

[T]he Commission henceforth will infer from evidence that a pretexter has obtained unauthorized access to a customer’s CPNI that the carrier did not sufficiently protect that customer’s CPNI.⁷

This inference was neither proposed by the Commission nor supported by any of the commenters.⁸ And that is for good reason. The presumption is inconsistent with the limits that the courts have placed on the use of such presumptions; it is incompatible with the enforcement

⁶ See, e.g., Memorandum Opinion and Order, *Filing and Review of Open Network Architecture Plans*, 4 FCC Rcd 1, 101-105 ¶¶ 398-415 (1988); Report and Order, *Policy and Rules Concerning Rates for Competitive Common Phase II Carrier Service and Facilities Authorizations Thereof*, 2 FCC Rcd 3072, 3093-98 ¶¶ 141-176 (1987); Report and Order, *Policy and Rules Concerning Rates for Competitive Common Carrier Services and Facilities Authorizations Thereof*, 104 F.C.C.2d 958, 1086-92 ¶¶ 256-265 (1986); Order, *Furnishing of Customer Premises Equipment and Enhanced Services by American Telephone & Telegraph Company*, 102 F.C.C.2d 655, 693-94 ¶ 66 (1985).

⁷ CPNI Order ¶ 63.

⁸ Cf. NPRM ¶ 26 (requesting comment on enforcement mechanisms); see, e.g., NASUCA Comments; EPIC Comments.

scheme established by Congress in the Communications Act; and it is at odds with the approach to similar legal duties consistently applied by other federal agencies and, indeed, by the Commission itself.

A. The Commission’s New Enforcement Presumption Would Be Unlawful.

It is well settled that an administrative agency may rely upon evidentiary presumptions.⁹ The Due Process Clause and the APA, however, place important limitations on the use of such presumptions.¹⁰ Here, the Commission’s apparent presumption would run afoul of these limitations by seeking to infer a legal conclusion from a fact, and by ignoring the requirement for a sound and rational basis for any such presumption.

First, courts will uphold the use by an agency of an evidentiary presumption only where there is a rational connection “between the *fact* proved and the ultimate *fact* presumed....”¹¹ Unlike typical evidentiary presumptions drawing connections between “two concrete *facts*,”¹² however, presumptions connecting a fact to a *legal* conclusion (where culpability is an issue) are problematic. As the D.C. Circuit has explained, “[d]istinctions between accidental, negligent, reckless, and intentional conduct ... make all the difference between an innocent act and a citable offense....”¹³ Consider the following example: If one were to see a car on the side of the road

⁹ See, e.g., *Chemical Mfrs. Ass’n v. Department of Transp.*, 105 F.3d 702, 705 (D.C. Cir. 1997).

¹⁰ See *Mobile, Jackson & Kansas City R.R. Co. v. Turnipseed*, 219 U.S. 35, 43 (1910); 5 U.S.C. § 556(d)..

¹¹ *Turnipseed*, 219 U.S. at 43 (emphasis added); *Chemical Mfrs.*, 105 F.3d at 705 (citing *Turnipseed*).

¹² *Secretary of Labor v. Keystone Coal Mining Corp.*, 151 F.3d 1096, 1102 (D.C. Cir. 1998) (emphasis in original).

¹³ *Id.* (invalidating a presumption between a fact and an intentional act).

with its front end badly damaged and smoke coming out of the radiator, it would be entirely rational to infer that the driver had been in an automobile accident. That is, it would be rational to infer one fact (that he had been in an accident) from another fact (that he was in his badly damaged car on the side of the road). But it would not be rational to infer that he had driven negligently (*i.e.*, had failed to exercise his duty to take reasonable measures) simply because he had been in an accident. He might well have driven negligently, but then again he might not have. There is simply no way to tell until the matter has been fully and properly adjudicated.

Applied here, these principles illustrate why the Commission's apparent presumption would be unlawful and inappropriate. To be sure, if there were a breach of a customer's CPNI – whether by a pretexter or by some other party – that would be an unacceptable invasion of the customer's privacy. But there is simply no rational basis to make even preliminary assessments of the level of fault of the carrier, if any, based on the fact that there has been a breach. Indeed, as the Commission's order recognizes, carriers have strong incentives to protect their customers' privacy, and pretexting itself involves the tortious (and possibly criminal) acts of a third party. Simply the act by the pretexter of successfully securing customer information through fraud and misrepresentation does not identify how the information was obtained, or what role the carrier played in its disclosure. Accordingly, the judicial reluctance to accept such agency presumptions seems well placed in this context, particularly when the pretexter likely is acting in a criminal manner. This judicial reluctance has clear analogies at common law. Tort law does not apply the doctrine of *res ipsa loquitur* unless “other responsible causes, including the conduct of ... third persons, are sufficiently eliminated by the evidence.”¹⁴ Thus, it is not possible to presume

¹⁴ Restatement (Second) of Torts § 328D(1)(b) (1965).

from the fact of an unauthorized disclosure that a carrier has not satisfied its legal obligation to take “reasonable measures” to protect CPNI.¹⁵

Second, even assuming that the Commission’s proposed presumption connected two *facts* (as opposed to a fact and a legal conclusion, as explained above), the presumption would still fail to meet the standards established by reviewing courts. Here, the presumption does not rely on a “sound and rational connection” between the proved and inferred facts.¹⁶ Courts require that “proof of one fact renders the existence of another fact ‘*so probable* that it is sensible and timesaving to assume the truth of [the inferred] fact ... until the adversary disproves it.’”¹⁷ On the other hand, “[i]f there is an *alternate explanation* for the evidence that is also *reasonably likely*, then the presumption is irrational.”¹⁸

Here, the Commission would have to have a rational basis for concluding that an unauthorized disclosure – standing alone, by itself – would render a carrier’s negligence “so probable that it is sensible and timesaving to assume” it and that no “reasonably likely” alternative explanation for the disclosure (*i.e.* other than carrier negligence) exists. But such an alternate explanation plainly *does* exist: through no negligence of its own, a carrier may still be victimized by a customer’s self-disclosure of key information, as well as by new, unanticipated,

¹⁵ See 47 C.F.R. § 64.2010(a) (as added by the *CPNI Order*). Moreover, the presumption’s use of the phrase “sufficiently protect” must be interpreted as referring to *legal* sufficiency, and not mere *factual* sufficiency, since the latter interpretation would turn the presumption into a meaningless truism.

¹⁶ *NLRB v. Baptist Hosp., Inc.*, 442 U.S. 773, 787 (1979); *Chemical Mfrs.* 105 F.3d at 705 (citing *Baptist Hosp.*).

¹⁷ *NLRB v. Curtin Matheson Scientific, Inc.*, 494 U.S. 775, 788-89 (1990) (quoting E. Cleary, McCormick on Evidence § 343, at 969 (3d ed. 1984)) (emphasis added) (alterations in original).

¹⁸ *Keystone Coal Mining Corp.*, 151 F.3d at 1101.

and more sophisticated methods of attack.¹⁹ The Commission itself has recognized that carriers face daunting challenges protecting CPNI, with the *CPNI Order* noting that “techniques for fraud . . . tend to become more sophisticated over time,” that “data brokers may respond by escalating their techniques,” and thus that carriers will need to learn from these “emerging threats.”²⁰

The evolving and highly sophisticated efforts of data brokers are not the only causes of unauthorized disclosure that may defeat reasonable security measures. As CTIA and others noted, some customers “freely share their passwords with significant others and family members, therefore compromising the security of their own accounts.”²¹ Such persons may well have a keen interest in obtaining CPNI “for extra-judicial discovery in matrimonial and other domestic matters.”²² It is not surprising that the Chair of the Federal Trade Commission has herself noted that it is simply impossible for carriers to protect against every conceivable *future* occurrence of unauthorized access with 100% success.²³

¹⁹ Cf. Gramm-Leach-Bliley Act § 501(b)(2), Pub. L. No. 106-102, 113 Stat. 1436, 1437, *codified at* 15 U.S.C. § 6801(b)(2) (requiring agencies to develop safeguards for financial institutions that “protect against any *anticipated* threats or hazards to the security or integrity of . . . records”) (emphasis added).

²⁰ *CPNI Order* ¶¶ 33, 36.

²¹ CTIA Reply Comments at 4-5; *see also* Sprint Nextel Comments at 10; Cingular Comments at 13.

²² CTIA Reply Comments at 4-5 n.12.

²³ *See, e.g.*, Remarks of Deborah Platt Majoras, Chair, FTC, at the U.S. Chamber of Commerce, Dec. 5, 2006, at 7 (“data security can be breached despite the best of security procedures”) (“Majoras Remarks”); *cf. Whirlpool Corp. v. OSHA*, 645 F.2d 1096, 1098 (D.C. Cir. 1981) (to establish a violation of the “general duty” clause, the agency must demonstrate, *inter alia*, “the existence of a feasible method of abatement.”). Under *Whirlpool*, the agency has the burden of coming forward with evidence on the feasibility issue. *Id.* This requirement is based in the “broad sweep of the [general duty] clause, for proof of the specific method of abatement . . . helps provide the employer with notice of the precise hazard at issue.” *Id.* (citations omitted).

Finally, the Commission's proposed presumption is not rational for yet another independent reason. The *CPNI Order* presumes negligence on the part of *all* carriers that have been involved in an unauthorized disclosure, whether the carriers complied with the Commission's various safeguards or not. In other words, the presumption in the *CPNI Order* fails to distinguish between carriers that are in compliance with the applicable safeguards and carriers that are not.²⁴ Surely it is relevant when assessing a carrier's culpability to know whether it complied with the Commission's own safeguards. In this regard, relying on a presumption now would also be premature, particularly given the lack of notice that the Commission was considering a presumption and the lack of support in the record.²⁵ The Commission's Further Notice has identified additional steps (such as audit trails and physical safeguards) that may or may not be reasonable and appropriate steps to require data protection. How can the Commission presume that a carrier has failed to take "reasonable measures" when it has not even yet determined itself what measures are appropriate?

In the end, the presumption fails to acknowledge that carriers are as much victims of pretexting as are the affected customers: carriers are subject to reputational and potentially direct financial loss as a result of breaches and have therefore been among the most aggressive in bringing private actions against pretexters.²⁶

²⁴ Cf. *GTE Service Corp. v. FCC*, 205 F.3d 416, 422 (D.C. Cir. 2000) (finding aspects of the Commission's *Collocation Order*, 14 FCC Rcd 4761 (1999), to be "overly broad and disconnected from the statutory purpose enunciated"); *Troy Corp. v. Browner*, 120 F.3d 277, 285 (D.C. Cir. 1997) (noting that an agency's interpretation must be "reasonable and consistent with the statutory purpose").

²⁵ See *supra* note 8.

²⁶ See *CPNI Order* ¶ 12.

B. A Presumption Would Be Inconsistent With The Enforcement Regime In The Communications Act.

If the Commission were to rely on a presumption, it would also create a needless inconsistency with the Act's enforcement regime. In the case of an alleged violation of Section 222, the Act places the burden of persuasion – that is, the burden to persuade the decision maker that there has been a violation – on the charging party. Whether through the Section 208 complaint mechanism or through a forfeiture proceeding under Section 503, the ultimate burden of proof to prove a violation lies with the complainant or the Commission respectively, not with carriers.²⁷

But here, in apparent service of the enforcement presumption, the *CPNI Order* has flipped the burden of persuasion and placed it on the carrier – without raising the issue in the NPRM or providing an opportunity for commenters to respond. It is now the carrier that “*must demonstrate that ... [its] policies and procedures are reasonable*”²⁸ in order to avoid liability. This impermissibly shifts the “ultimate burden of proof in the sense of [which side bears] the risk of nonpersuasion” from the Commission (or a third party) to the carriers.²⁹ And while Congress itself may shift the burden of persuasion,³⁰ it did not do so when enacting Section 222 of the

²⁷ See *Hi-Tech Furnace Sys., Inc. v. FCC*, 224 F.3d 781, 787 (D.C. Cir. 2000) (affirming that the complainant in a proceeding conducted under section 208 of the Act bears the burden of proof); 47 U.S.C. § 504(a) (requiring a *trial de novo* to enforce forfeiture penalties, in which the government – as plaintiff – would retain the burden of persuasion).

²⁸ *CPNI Order* ¶ 63 (emphasis added).

²⁹ See *Chemical Mfrs.*, 105 F.3d at 706.

³⁰ See *General Elec. Co. v. United States Dep't of Commerce*, 128 F.3d 767, 771-772 (D.C. Cir. 1997); *United Scenic Artists, Local 829 v. NLRB*, 762 F.2d. 1027, 1034 (D.C. Cir. 1985).

Communications Act.³¹ And it is well settled that an evidentiary presumption may not shift the burden of persuasion.³² Doing so here would be inconsistent with the enforcement scheme as mandated by Congress in the Act.

The use of a presumption is particularly inappropriate in light of the unique interplay of the “willfulness” requirement of Title V of the Act with the kind of legal duty at issue here. A bedrock principle of Section 503 of the Act is that a carrier’s violation of the Commission’s rules cannot be punished unless it is “willful” or “repeated.”³³ Congress defined the term “willful” to mean the “*conscious and deliberate commission or omission of such act*, irrespective of any intent to violate any [rule, regulation, or statute].”³⁴ Congress and the Commission further

³¹ Section 222 created a general duty for carriers to protect CPNI. *See* 47 U.S.C. § 222(a); *CPNI Order* n. 6 (“Section 222(a) imposes a *general* duty on telecommunications carriers....”) (emphasis added). This does not create strict liability, *e.g.* the elimination of any need for the Commission to prove a breach of the duty of care. In *Whirlpool Corp.*, 645 F.2d 1096, the D.C. Circuit affirmed that the Occupational Health and Safety Act’s “general duty” clause – requiring employers to furnish a safe workplace – “does not impose strict liability on employers, but instead limits their liability to ‘preventable hazards.’” *Id.* at 1098; *see also* 29 U.S.C. § 654(a)(1).

³² *See* 5 U.S.C. § 556(d); *Department of Labor v. Greenwich Collieries*, 512 U.S. 267, 278-281 (1994); *National Mining Ass’n v. Babbitt*, 172 F.3d 906, 910 (D.C. Cir. 1999). A presumption may lawfully shift the burden of *production*, which is an evidentiary obligation to introduce enough evidence on an issue to have the issue decided by the fact-finder. Black’s Law Dictionary at 1223 (8th ed. 2004). This burden may shift between parties during the course of a proceeding. The ultimate burden of *persuasion*, by contrast, is an obligation that remains on a single party throughout a proceeding to satisfy the legal elements of a claim by convincing the fact-finder to view the facts in a way that favors that party. *See id.* at 209.

³³ 47 U.S.C. § 503(b)(1)(B). Notably, Congress considered and specifically rejected a mere negligence standard under Section 503. *See* S. Rep. No. 1857 at 8-9 (1960).

³⁴ 47 U.S.C. § 312(f); *see* Communications Amendments Act of 1982 § 117, Pub. L. No. 97-259, 96 Stat. 1087, 1095 (adding Sec. 312(f)); H.R. Conf. Rep. No. 97-765 at 50-51, *reprinted at* 1982 U.S.C.C.A.N. 2261, 2294-95 (“1982 Conference Report”) (noting that this definition is also intended to apply in Sec. 503).

clarified that “‘willful’ means that the licensee *knew* that he was doing the act in question, regardless of whether there was an intent to violate the law.”³⁵

In a typical enforcement case, the “act” in question is a violation of a specific proscriptive legal obligation (*i.e.*, failure to implement the password requirement or failure to ask for photo ID at a retail location). Here, however, the relevant legal obligation is a legal duty whose scope will necessarily vary given the facts and circumstances of a particular case – the obligation to take “reasonable measures” to protect CPNI. Thus, to impose a forfeiture on carriers under the new CPNI rules, the Commission must prove a “conscious and deliberate ... omission” by carriers of “reasonable measures” to protect CPNI.³⁶ Similarly, under the clarified formulation, “willful” means that the carrier knew that it was doing the act in question, *i.e.* that the carrier *knew* it was failing to take reasonable measures to protect CPNI.³⁷

The Commission’s presumption of carrier liability based on an unauthorized disclosure to a pretexter is therefore particularly incompatible with the Commission’s enforcement regime, for the simple reason that a carrier cannot consciously know – in advance of every breach – that it is failing to take all “reasonable measures” necessary. As stated above, the Commission itself has recognized that pretexters are constantly growing more sophisticated, and that carriers are constantly learning about “emerging threats.”³⁸ And there is no apparent way to defend against

³⁵ 1982 Conference Report at 51; Memorandum Opinion and Order, *Application for Review of Southern California Broadcasting Company Licensee, Radio Station KIEV(AM) Glendale, California*, 6 FCC Rcd 4387-88 ¶ 5 (1991) (citing the 1982 Conference Report).

³⁶ See 47 U.S.C. § 312(f); 47 C.F.R. § 64.2010(a) (as added by the *CPNI Order*).

³⁷ The issue of intent, frequently (and mistakenly) raised as a defense before the Commission, never arises in situations where, as here, no “conscious and deliberate . . . omission” has occurred.

³⁸ See p. 9 *supra*.

unauthorized access to passwords by other family members. Thus, if the facts show that the breach was not reasonably foreseeable or preventable, it cannot be presumptively deemed to be a “willful” violation of the Act.

C. The Presumption Would Be Inconsistent With The Practice Of The Commission And Other Agencies.

A presumption that a carrier acted unreasonably in the event of *any* breach is inconsistent with approaches to data security previously adopted by other agencies, and with approaches to liability previously taken by the Commission itself. Drawing upon well-established principles of tort law,³⁹ the typical approach involves a balance between the likelihood of unauthorized access, the extent of the harm, the feasibility of additional measures, and whether the cost is reasonable given the technology a carrier already has implemented – principles the Commission recognized in the *CPNI Order*.⁴⁰ For example, the FTC’s Safeguards Rule was based on principles outlined by an expert panel,⁴¹ which sought to “balanc[e] the sometimes-competing considerations of security, costs, and privacy.”⁴² Accordingly, it requires financial institutions to

³⁹ In applying the duty to exercise reasonable care under negligence law, courts routinely weigh “(1) the magnitude of the risk and (2) the gravity of the risk against (3) the utility of the defendant’s conduct and the costs of making it safer.” Dan B. Dobbs, *THE LAW OF TORTS* § 144 (2000); *see also* Restatement 2d of Torts § 291 (1965) (negligence if the magnitude of the risk outweighs the utility of the defendant’s conduct); *United States v. Carroll Towing Co.*, 159 F.2d 169, 173 (2d Cir. 1947) (Hand, J.) (duty depends on a formula taking into account (1) the probability of injury, (2) the gravity of the resulting injury, and (3) the burden of taking adequate precautions).

⁴⁰ *See CPNI Order* ¶¶ 64-65; *see also* Statement of Commissioner Robert M. McDowell (the Commission’s rules “should strike a careful balance and should also guard against imposing over-reaching and unnecessary requirements that could cause unjustified burdens and costs on carriers”).

⁴¹ *See* 67 Fed. Reg. 36484 n. 6 (2002) (noting the FTC’s consideration of the Final Report of its Advisory Committee on Online Access and Security, May 15, 2000, (“FTC Advisory Committee Report”), *available at* <http://www.ftc.gov/acoas/papers/finalreport.htm>).

⁴² FTC Advisory Committee Report at § 3.1.

implement “administrative, technical, and physical safeguards that are appropriate to [an institution’s] size and complexity, the nature and scope of [its] activities, and the sensitivity of any customer information at issue.”⁴³ The same is true in cases brought by the FTC under Section 5 of the Federal Trade Commission Act⁴⁴ with respect to the security of personally identifiable information that is certainly no less sensitive than telephone call records (*e.g.*, credit card information that can lead to identity theft). In those cases, the FTC has recognized the need to inquire whether a claimed “failure to employ reasonable and appropriate security measures” is “offset by countervailing benefits to consumers or competition,”⁴⁵ and/or whether companies failed to implement “simple, low-cost, and readily available defenses.”⁴⁶

The same is true of other agencies as well. The Office of the Comptroller of the Currency, the Federal Reserve, the FDIC, the Office of Thrift Supervision, and the National Credit Union Administration all have recognized that certain security measures – even if they might prevent a small number of unauthorized disclosures – are not reasonable or required

⁴³ 16 C.F.R. § 314.3(a). The Safeguards Rule implements sections 501 and 505(b)(2) of the Gramm-Leach-Bliley Act. 16 C.F.R. § 314.1(a); *see also* n. 19 above.

⁴⁴ 15 U.S.C. § 45(a)(1) (prohibiting “unfair or deceptive” trade practices).

⁴⁵ *See, e.g.*, FTC Decision, BJs Wholesale, Dkt. No. C-4148 ¶ 9 (2005); FTC Decision, DSW Inc., Dkt. No. C-4157 ¶ 10 (2006) (same).

⁴⁶ *See, e.g.*, FTC Decision, Guidance Software, Inc., Dkt. No. C-4187 ¶ 8 (2007); FTC Decision, CardSystems Solutions, Inc., Dkt. No. C-4168 ¶ 6 (2006) (same).

because of cost, feasibility, or other considerations.⁴⁷ Instead of relying on a presumption of guilt, these agencies have instead mandated a programmatic approach to security, requiring, *inter alia*, that institutions conduct risk assessments of *reasonably foreseeable* threats and manage and control risks appropriately.⁴⁸ Indeed, the agencies specifically opposed a “standard of absolute liability for a financial institution that experiences a security breach,” and accordingly clarified the objectives of their regulations “by stating that each security program is to be *designed* to accomplish the objectives stated.”⁴⁹

The enforcement presumption is not just inconsistent with approaches taken by other agencies; it is also inconsistent with approaches the Commission itself has taken. For example, in implementing the national “do-not-call” registry, the Commission did not rely on an enforcement presumption. It instead established a set of programmatic requirements, including written procedures, training of personnel, and accessing the do-not-call list no more than 31 days prior to any call.⁵⁰ Similarly, the Commission has not relied on a presumption in implementing Section 317’s requirement that a licensee exercise “reasonable diligence” to obtain information

⁴⁷ See, e.g., *Interagency Guidelines Establishing Standards for Safeguarding Customer Information*, 66 Fed. Reg. 8616, 8626 (Feb. 1, 2001) (“Interagency Guidelines”) (to “minimize the economic impact” on businesses, the rule allows each institution “the discretion to design an information security program that suits its particular size and complexity,” rejects “more proscriptive guidelines” since they would be “more burdensome,” and only identifies security measures that are “likely to have the greatest applicability”) (“Interagency Guidelines”); *id.* at 8627 (“an institution must determine for itself which measures will be appropriate for its own risk profile”); see also FTC Advisory Committee Report at § 3.1.

⁴⁸ See, e.g., *Interagency Guidelines* Sec. III-B, C, *codified*, e.g., at 12 C.F.R. Part 30 App. B, *id.* at Part 208 App. D-2, *id.* at Part 225 App. F, *id.* at Part 364 App. B, *id.* at Part 570 App. B.

⁴⁹ *Interagency Guidelines*, 66 Fed. Reg. at 8620 (emphasis in original).

⁵⁰ See 47 C.F.R. § 64.1200(c)(2)(i).

concerning sponsorship identification.⁵¹ Indeed, the Commission has explained that it would not place a licensee in the position of being an “insurer,” *i.e.*, strictly liable for any failure to make the required identification.⁵²

In the end, none of these situations involved a presumption of liability in the event of unauthorized disclosure. As FTC Chairman Majoras has recognized, “[r]easonableness does not mean perfection, of course; data security can be breached despite the best of security procedures.”⁵³ Thus, “the fact that a company suffered a breach does not, in and of itself, establish that its practices were unreasonable....”⁵⁴ To be sure, carriers should take every step reasonable to ensure that CPNI is not breached, and CTIA shares the Commission’s objectives. But any attempt to establish a standard of perfection would only lead to a misallocation of resources in a futile effort to achieve the standard. This would only harm, not serve, the public interest. For the reasons detailed above, the Commission should reconsider its decision establishing the presumption.

II. THE COMMISSION SHOULD PROVIDE FURTHER GUIDANCE CONCERNING “REASONABLE MEASURES.”

In implementing its new “reasonable measures” standard, the Commission stated that it expects carriers to take “additional steps” to protect CPNI “to the extent such measures are feasible for a particular carrier.”⁵⁵ Although a number of parties urged the Commission to make

⁵¹ 47 U.S.C. § 317(c).

⁵² Memorandum Opinion and Order, *Metroplex Communications, Inc.*, 5 FCC Rcd 5610 (1990).

⁵³ Majoras Remarks at 7.

⁵⁴ *Id.*

⁵⁵ *CPNI Order* ¶ 64.

clear what those steps should be by establishing a so-called “safe harbor,” in response to the suggestion in the Commission’s notice, the Commission ultimately opted against adopting such an approach. In particular, it refused to endorse as a safe harbor a set of “security guidelines . . . comparable to the [FTC’s] guidelines for the financial industry.” In the Commission’s view, these guidelines would “not add meaningful protections beyond carriers’ existing regulatory obligations,” and thus adoption of such a safe harbor “would result in less protection of customers’ CPNI than exists under the status quo.”⁵⁶

In order to further clarify carriers’ legal obligations under Section 222, the Commission should reconsider its apparent rejection of the value of such a programmatic approach. This approach has the benefit of requiring each carrier to adopt a comprehensive program designed to avoid unauthorized disclosure of CPNI in a way that is appropriate to its circumstances. The FTC’s rule, for example, does not establish a safe harbor. Rather, it includes a general obligation to “maintain a comprehensive information security program” whose safeguards “are appropriate to your size and complexity, the nature and scope of your activities, and the sensitivity of any customer information at issue,” and that is “reasonably designed to achieve the objectives” of the rules.⁵⁷ Instead of requiring only a series of specific safeguards (*e.g.*, passwords), it relies on five comprehensive and systematic requirements: (1) designation of an employee (or employees) responsible for coordinating the safeguards program; (2) identification of “reasonably foreseeable internal and external risks,” including in the areas of employee training and management, information systems, processing, storage, transmission, and disposal; (3) design and implementation of safeguards to control these risks and regular testing or monitoring of these

⁵⁶ CPNI Order ¶ 66.

⁵⁷ 16 C.F.R. § 314.3(a).

safeguards; (4) oversight of service providers; and (5) evaluation and adjustment of the program in light of the foregoing testing and monitoring.⁵⁸

Such general guidelines would serve the public interest by ensuring that each carrier adopts a data security program for CPNI that covers each of these critical bases, while at the same time providing no opportunity for evasion in cases of “egregious” conduct.⁵⁹ While unauthorized disclosure of CPNI due to a breach might well occur notwithstanding the implementation of such a program, and while the Commission could determine that the program in a particular case did not in fact comply with the foregoing guidelines, the good-faith efforts of a carrier to implement such a program should be relevant to any Commission inquiry into compliance with the “reasonable measures” obligation of the new rule. This approach would balance the need for guidance in implementing this new legal duty by carriers with the flexibility to examine the facts and circumstances of any individual case of unauthorized but inadvertent disclosure of CPNI.

III. THE COMMISSION SHOULD MODIFY ITS DEFINITION OF “ADDRESS OF RECORD.”

The *CPNI Order* now requires carriers to “immediately” notify their customers of account changes, such as whenever a password is changed, and permits such notification by “mail to the address of record,” among other methods.⁶⁰ While CTIA’s member carriers are

⁵⁸ 16 C.F.R. § 314.4.

⁵⁹ The record in this proceeding contains substantial evidence that the prospect of such “egregious” behavior is remote, given the market incentives of carriers to protect their customers from unauthorized disclosure as well as the existing state and federal law obligations to protect their personally identifiable information. However, as noted above, reliance on the obligation to adopt the kind of comprehensive security program contemplated by the FTC’s rule would not foreclose Commission enforcement action in such “egregious” cases.

⁶⁰ 47 C.F.R. § 64.2010(f).

willing to comply with this requirement, the new rules do not allow carriers the same options and flexibility to provide immediate notification to *new* customers as they do for longer-standing customers. The *CPNI Order* now defines a customer’s “address of record,” whether postal or electronic, to be an address associated with the customer’s account “for at least 30 days.”⁶¹ Therefore, any notification to a customer of an account change made within the first 30 days of service cannot be accomplished by “mail to the address of record,”⁶² since by definition no such “address of record” is recognized under the rules.

Additionally, carriers often assist customers who forget both their password and any “shared secret” backup data by using postal or electronic mail to the “address of record” for re-authentication.⁶³ However, such re-authentication would be impossible within the first 30 days of service, preventing any further assistance by the carrier to the customer during the initial period. New customers demand an even higher level of service at the onset of the relationship as they become familiar with features and services. Thus, it is especially important for carriers to have the flexibility to notify new customers in a way that makes the most sense for the customer.

To avoid these problems, the Commission should modify its definition of “address of record” as follows:

Address of record. An “address of record,” whether postal or electronic, is an address that the carrier has associated with the customer’s account for at least 30 days; and, for the first 30 days following account establishment, is an address that the carrier has associated with the customer’s account upon activation of service.

This modest modification would solve the problems discussed above, while not reducing any protections against pretexters. The Commission adopted the 30-day rule to “foreclose a

⁶¹ 47 C.F.R. § 64.2003(b).

⁶² 47 C.F.R. § 64.2010(f).

⁶³ See 47 C.F.R. § 64.2010(e).

pretexter's ability to change an address of record for the purpose of being sent call detail information immediately."⁶⁴ By restricting the rule modification above to the address associated with initial account activation, the rule would still prevent a pretexter from being able to change an account address within the first 30 days of service and immediately obtain call-detail information at the new address.

IV. THE COMMISSION SHOULD CLARIFY THAT MULTIPLE CPNI CERTIFICATIONS ARE NOT REQUIRED FOR 2007.

Public notice of the *CPNI Order* occurred upon publication in the Federal Register on June 8, 2007.⁶⁵ The rules are scheduled to take effect six months following that date – December 8, 2007 – or upon OMB approval of the new information-collection requirements, whichever is later.⁶⁶ The effective date triggers the obligation under the *CPNI Order* for carriers to file their annual CPNI certification – a filing that now includes an explanation of all actions taken against data brokers and a summary of all complaints received in the past year.⁶⁷ The certification required under the *CPNI Order* must be filed for data pertaining to the “previous calendar year,”⁶⁸ creating a seemingly inadvertent requirement for carriers to prepare and file a separate CPNI certification for the interim period from December 8 through December 31, 2007 under the new rules. This second certification would be in addition to any certification prepared under the existing rule for the period from January 1 to December 7, 2007.

⁶⁴ *CPNI Order* n. 46.

⁶⁵ 72 Fed. Reg. 31,948 (June 8, 2007).

⁶⁶ *See CPNI Order* ¶ 84.

⁶⁷ *See* 47 C.F.R. § 64.2009(e) (as amended); *see also* 72 Fed. Reg. 31948 (noting that the revisions to Sec. 64.2009(e) are among those for which OMB approval is required).

⁶⁸ 47 C.F.R. § 64.2009(e).

The preparation of an additional CPNI certification under the new rules solely to cover a short period in December after the new rules are effective would needlessly burden carriers, while providing very minimal value to the Commission in terms of “monitor[ing] the industry’s response to CPNI privacy issues.”⁶⁹ The Commission should therefore clarify that if OMB approval occurs in 2007, any data for the final weeks of 2007 may be incorporated into the annual filing required for 2008. Thus, the 2007 certification would be for the period January 1, 2007 through December 7, 2007 (or the date of OMB approval if later), and the 2008 certification under the new rules would be for the period December 8, 2007 through December 31, 2008. Should OMB approval not occur until 2008, the certification for that year would include data for the period beginning on the date of such approval.

V. THE COMMISSION SHOULD CLARIFY THAT ITS RULE FOR TELEPHONE ACCESS TO CPNI ONLY APPLIES TO CUSTOMER-INITIATED CONTACT.

The Commission’s new rule governing telephone access to CPNI appears to be appropriately targeted at the release of call-detail information based on customer-initiated telephone contact.⁷⁰ However, some of the language adopted in the rule is ambiguous, and it could be misconstrued to encompass telephone contact initiated by the carrier. Disclosure of CPNI is occasionally necessary during a carrier-initiated call to a customer at an alternate telephone number, e.g., when there are technical issues preventing contact at the primary telephone number of record or when contacting a customer about a final bill after the customer has left the carrier. In such circumstances, the carrier may use a “preferred” contact number on file instead of the primary “telephone number of record.”

⁶⁹ CPNI Order ¶ 51. Furthermore, there is certainly no need to “remind carriers,” at least this year, “of the Commission’s oversight and high priority regarding carrier performance in this area” by requiring a separate filing for a 24-day period at the end of the year. *See id.*

⁷⁰ *See* 47 C.F.R. § 64.2010(b).

To solve this problem, the Commission should slightly modify one sentence in its telephone access rule by clarifying that the sentence – like the remainder of the rule – only applies to customer-initiated telephone requests for CPNI:

Telecommunications carriers may only disclose call detail information over the telephone, based on customer-initiated telephone contact, if the customer first provides the carrier with a password, as described in paragraph (e) of this section, that is not prompted by the carrier asking for readily available biographical information, or account information. If the customer does not provide a password, the telecommunications carrier may only disclose call detail information in response to a customer-initiated call by sending it to the customer's address of record, or, by calling the customer at the telephone number of record. If the customer is able to provide call detail information to the telecommunications carrier during a customer-initiated call without the telecommunications carrier's assistance, then the telecommunications carrier is permitted to discuss the call detail information provided by the customer.⁷¹

This modest change conforms to the remainder of the paragraph, fully reflects the *CPNI Order's* intent to provide protections against the disclosure of call-detail information based on customer-initiated telephone contact,⁷² and does not undermine the Commission's laudable efforts to protect consumers from pretexters.

CONCLUSION

For the foregoing reasons, we respectfully request that the Commission reconsider its CPNI Order by taking the following steps: (1) Eliminate any presumption that an unauthorized disclosure means that the carrier did not take "reasonable measures" to avoid pretexting. (2) Provide additional guidance concerning the kinds of security program it expects carriers to implement to meet the "reasonable measures" standard. (3) Modify its definition of "address of record" by allowing carriers to provide assistance to customers within the first 30 days after service is initiated. (4) Clarify that a separate CPNI certification under the new rules for the final

⁷¹ 47 C.F.R. § 64.2010(b) (as added by the *CPNI Order*, with CTIA's suggested modification underlined.)

⁷² See *CPNI Order* § IV-A-1 (entitled Customer-Initiated Telephone Account Access).

weeks of 2007 is unnecessary and can be included instead along with the certification for 2008.

(5) Clarify that the rule governing telephone access to call-detail information only applies to customer-initiated telephone contact.

Respectfully submitted,

/s/ Michael F. Altschul

Michael F. Altschul
Senior Vice President, General Counsel

Christopher Guttman-McCabe
Vice President, Regulatory Affairs

Paul W. Garnett
Assistant Vice President, Regulatory Affairs

Brian M. Josef
Director, Regulatory Affairs

CTIA – The Wireless Association®
1400 16th Street, NW, Suite 600
Washington, DC 20036
(202)-785-0081

July 9, 2007