

**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 |

**COMMENTS OF
THE UNITED STATES TELECOM ASSOCIATION**

INTRODUCTION

As consumers increasingly switch their voice service business among wireline telecommunications companies, cable companies, wireless companies, and VoIP companies, providing efficient customer service that meets customer expectations has become a business essential. One essential expectation that consumers have is that their personal information will be properly protected. In today's busy world, another key expectation is that consumers will have easy and efficient access to their accounts to add or subtract features and services and to obtain billing information. In today's market, every carrier has to balance these competing customer demands with the need to provide service efficiently in developing a customer service experience that will give their business a competitive advantage.

The Federal Communication Commission's recent order regarding customer proprietary network information (CPNI) imposes a set of new obligations on communications providers governing aspects of the customer relationship. In its Report

and Order and Further Notice of Proposed Rulemaking (the CPNI Order),¹ the Commission attempted to crack down on pretexting by requiring telecommunications carriers to implement safeguards aimed at protecting CPNI. In the further notice, the Commission asked whether it should require optional or mandatory password protection for non-call detail CPNI and whether it should adopt rules pertinent to audit trails, rules governing the physical transfer of CPNI, or rules requiring carriers to limit data retention.² The United States Telecom Association (USTelecom)³ strongly urges the Commission not to adopt any additional measures until the Commission has gained substantial experience with the operation of its recent new rules and can assess the consumer costs and benefits of those rules. Carriers and the public have no experience with the new rules. Until the rules have been implemented and tested to see whether they are sufficient to ensure the protection of customer privacy, there is no need to impose additional rules. Additional rules could be burdensome for consumers by making it more difficult to access account information than consumers would prefer and costly for

¹ *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information; IP-Enabled Services*, CC Docket No. 96-115, WC Docket No. 04-36, Report and Order and Further Notice of Proposed Rulemaking (rel. April 2, 2007).

² See CPNI Order ¶¶ 68-71.

³ USTelecom is the premier trade association representing service providers and suppliers for the telecommunications industry. USTelecom members provide a full array of services, including broadband, voice, data, and video over wireline and wireless networks.

carriers. Since there is no current evidence that further regulation would provide a consumer benefit, the Commission should refrain from imposing more regulation.

DISCUSSION

Protecting consumer privacy is of utmost concern to USTelecom members. It is an essential component of customer care for carriers' businesses and an unequivocal component of existing law. USTelecom members take their obligation to protect customer privacy seriously and devote significant resources to implementing and observing strict security protocols. Furthermore, there is no evidence that use of CPNI for marketing purposes has created security vulnerabilities. For these reasons, the Commission need not impose additional regulations on carriers.

Additional regulation would frustrate consumers by making it more difficult for them to efficiently access their accounts, change services, and obtain billing information. Furthermore, additional regulation would increase carriers' administrative costs and, ultimately, the cost of service to consumers. The new CPNI rules are not yet in effect and have not yet been tested. Until it has evidence of the effectiveness of the new regulations and of the need for additional regulation, the Commission should resist imposing additional regulation.

Requiring password protection for non-call detail CPNI would likely anger and annoy many customers while failing to provide any additional privacy protection. Non-call detail CPNI, such as the type of plan or billing method a customer chooses, is not the information sought by pretexters. Customers call customer service only occasionally and often cannot remember passwords. (In fact, most customers do not want passwords for customer service calls. Many USTelecom member companies offer their customers

password protection, but only a tiny fraction of customers accept them.) Requiring customers to provide passwords even when they are seeking information that pretexters do not care about would not protect them from any harmful activities and would serve only to frustrate and confuse them. Frustrated customers often spend longer periods with customer service representatives, which increases costs for companies. In addition, using passwords in a call center would not necessarily provide the same level of security that we typically associate with passwords used for online account access, where access and password retrieval are automated. Finally, requiring passwords for non-call detail CPNI would impose operational costs on companies that would have to do systems modifications and operator training. The increased operational costs and customer confusion resulting from passwords for non-call detail CPNI combined with the potential vulnerabilities created by use of passwords in call centers outweigh any perceived benefits to customers.

Similarly, audit trails would require significant systems modifications and costs without any corresponding consumer benefit. USTelecom does not have current estimates, but the last time the Commission considered requiring audit trails in the late 1990s, the cost of complying with the audit trail requirement was estimated to be \$270 million by legacy AT&T.⁴ BellSouth estimated that it would cost at least \$75 million to create a computer system to comply with the audit trail requirement.⁵ Small rural carriers

⁴ *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information; IP-Enabled Services*, CC Docket No. 96-115, WC Docket No. 04-36, Order on Reconsideration and Petitions for Forbearance at ¶ 123 (rel. Sept. 3, 1999).

⁵ *Id.*

estimated that the additional cost of compliance could range from \$12-\$64 per line.⁶ An audit trail mandate would get factored into the cost of doing business and eventually affect the price consumers pay for their service with no obvious benefit. The Commission itself has recognized this, saying, “Our current record indicates that the broad use of audit trails likely would be of limited value in ending pretexting because such a log would record enormous amounts of data, the vast majority of it being legitimate consumer inquiry.”⁷

Like rules requiring audit trails, rules governing the physical transfer of CPNI among companies, such as carriers and their affiliates or joint venture partners and independent contractors, would impose operational costs and administrative burdens without promising any corresponding benefit. Carriers already require third parties to enter into strict confidentiality agreements. As it has said before, USTelecom is not aware of any evidence that joint venture partners, independent contractors, or other third-party marketers used by its members have misused any CPNI shared with them, and the law already imposes strict privacy safeguarding requirements on marketers.⁸ Furthermore, third-party marketers know that they will put themselves out of business if they misuse CPNI. Mandating the way companies physically safeguard the confidentiality of CPNI then is unnecessary and unduly burdensome.

⁶ *Id.* at ¶ 124.

⁷ CPNI Order ¶ 69.

⁸ *See* letter from Indra Sehdev Chalk, Counsel, USTelecom, to Marlene H. Dortch, Secretary, FCC, CC Docket No. 96-115 (filed March 8, 2007).

Finally, the Commission should not mandate data retention limitations. CPNI is a broad term that encompasses different types of information, and, therefore, what to retain and for how long varies with the particular data at issue. For example, call detail records are relevant for tax purposes, so carriers must comply with a host of federal rules and regulations (including Internal Revenue Service rules and Sarbanes-Oxley requirements) as well as state rules and regulations to develop appropriate retention parameters for these records. FCC-imposed limitations on data retention could expose carriers to liability if they cannot maintain records as required by applicable state and federal statutes of limitations. Therefore, the Commission should not add another layer of regulation to the already effective state and federal regulation in this area.

Additional CPNI mandates would be particularly harmful to business customers because, unlike most residential customers, businesses typically are able to negotiate appropriate protection of CPNI in their service agreements with carriers.⁹ Also, data brokers and pretexters seem to target residential customers rather than business customers. The exception for business customers in the CPNI Order does not go far enough because it does not cover all business customers—only those serviced by a dedicated account representative as the primary contact.¹⁰ Because businesses can negotiate the level of CPNI protection they require, the exception should apply more broadly than just to large companies that do not use call centers.

⁹ See CPNI Order ¶25 n. 90.

¹⁰ CPNI Order ¶25. If the business customer must go through a call center to reach a customer service representative, then this exception does not apply to that customer. *Id.* n. 90.

CONCLUSION

Protecting consumer privacy is an essential component of customer care for USTelecom members. While USTelecom members devote significant resources to protecting customer privacy and support Commission efforts to protect customer privacy, additional CPNI rules are not warranted at this time. Until the Commission sees whether the consumer protections it implemented in the CPNI Order are effective, and what the costs and benefits of those rules are, it should not burden carriers and consumers with additional regulations—as the best approach to balancing customer needs for privacy and security with ease of access and efficiency is to let the market do its job.

Respectfully submitted,

UNITED STATES TELECOM ASSOCIATION

By: _____



Jonathan Banks
Indra Sehdev Chalk

Its Attorneys

607 14th Street, NW, Suite 400
Washington, DC 20005
(202) 326-7300

July 9, 2007