

**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;)	
)	
Petition for Rulemaking to Enhance Security and Authentication Standards for Access to Customer Proprietary Network Information)	RM-11277
)	

To: The Commission

COMMENTS OF RURAL CELLULAR ASSOCIATION

Rural Cellular Association (“RCA”)¹, by its attorneys, respectfully submits its comments filed in response to the Commission’s Notice of Proposed Rulemaking in the above-captioned proceeding seeking input on steps the Commission should take to further protect the privacy of customer proprietary network information (“CPNI”) that is collected and held by telecommunications carriers. *See Notice of Proposed Rulemaking*, CC Docket No. 96-115, RM-11277, released February 14, 2006 (“NPRM”). The proceeding, commenced in response to the petition filed by the Electronic Privacy Information Center (“EPIC”), is intended to determine whether the Commission should impose enhanced security and authentication standards for access to customer telephone records. RCA opposes imposition of additional regulatory burdens in this regard, particularly as they may be applied to small and regional wireless

¹ RCA is an association representing the interests of nearly 100 small and rural wireless licensees providing commercial services to subscribers throughout the nation. Its member companies provide service in more than 135 rural and small metropolitan markets where approximately 14.6 million people reside. RCA was formed in 1993 to address the distinctive issues facing wireless service providers.

carriers.²

I. Existing Safeguards are Sufficient to Protect CPNI

Section 222 of the Communications Act provides the framework for protection of CPNI.³ Section 222 defines CPNI and provides the parameters for its legitimate use. The FCC has further refined restrictions on use of CPNI and means of obtaining customer consent for its use. The FCC has extensively codified safeguards to protect against unauthorized use or disclosure of CPNI. For example, FCC rules require carriers to design their customer service records in such a way that the status of a customer's CPNI approval can be clearly established; to train personnel as to when they are and are not authorized to use CPNI; to have an express disciplinary process in place; to maintain records tracking access to customer CPNI records; to maintain a record of all instances where CPNI is disclosed to, provided to or accessed by third parties; to maintain such records for a period of at least one year; to establish a supervisory review process for outbound marketing campaigns; to certify annually regarding compliance with the CPNI requirements and to make this certification publicly available.⁴

II. Additional Security Measures Would Impose Costs not Justified by Experience

Now under consideration is the petition of EPIC, who proposes five forms of security measures to more adequately protect access to CPNI: consumer-set passwords, audit trails, encryption, limiting data retention, and notice procedures. RCA will comment below on the

² RCA's wireless carriers operate in rural markets and in a few small metropolitan areas. No member has as many as 1 million customers, and the vast majority of RCA's members serve fewer than 500,000 customers.

³ See 47 U.S.C. § 222, Telecommunications Act of 1996, Pub. L. No. 104-104, 110 Stat. 56 (codified at 47 U.S.C. §§ 151 *et seq.*).

⁴ See 47 C.F.R. § 64.2009; *see also CPNI Order*, 13 FCC Rcd at 8195, para. 193, *et seq.* (1998); *see also Order on Reconsideration and Petitions for Forbearance*, 14 FCC Rcd 14409, 14468 n. 331 (1999).

feasibility and advisability of these and other measures.

1. Consumer-Set Passwords

While consumer-set passwords and “shared secrets” techniques can increase the security of CPNI, requiring carriers to adopt such systems may aggravate customers who do not wish to remember a password, who have to take steps to retrieve a forgotten password, and who may be discouraged from dealing with the carrier due to the password obstacle. Passwords should not be a requirement, particularly not for small and regional carriers. Such carriers can protect CPNI in ways better than forcing subscribers to remember passwords and secrets. Passwords are useful for customers who prefer to manage accounts online, and most carriers who offer online account access provide the password feature. Considering the costs and disadvantages of passwords, the choice of whether and when to implement password systems should be left to the carrier.

2. Audit Trails

EPIC suggests that the FCC require carriers to record all instances when a customer’s records have been accessed, whether information was disclosed, and to whom. This would exceed the Commission’s existing rule requirement that carriers record any CPNI disclosure for use in marketing or to third parties. It could extend to include disclosure of CPNI to account holders. RCA believes such audit requirements would be costly and time consuming. Importantly, they would not make CPNI any more secure than it already is. Audit trails do not prevent unlawful disclosure. Requiring carriers to augment recordkeeping for this purpose would impose an unnecessary cost for negligible benefit.

3. Encryption

Encrypting all stored records would hugely increase the operating costs of small and regional carriers without enhancing the protection of CPNI. Stored records are not traditionally

vulnerable to persons who seek illegitimate access to CPNI. Small and regional carriers have existing controls over access to stored data by personnel. Customers have no access to stored data. Requiring encryption of records that are already secure would not advance the cause of CPNI protection, but it would add significantly to the burdens on carriers.

4. Limiting Date Retention

The required destruction of call records when they are no longer needed for billing or dispute purposes is not as practical as it sounds. There is no sure way to know when a record will no longer be relevant to a contested situation, law enforcement or other proceeding. Furthermore, like stored data, call records are not easily subject to pilfering of CPNI. Access is extremely limited. Enforced limitation of call retention data is not likely to make CPNI more secure. It will only add to regulatory costs and burdens.

5. Notice

EPIC suggests that companies notify customers when the security of their CPNI may have been breached. Notification could apply even to incidents where the carrier has no grounds to suspect that the request for CPNI was not legitimate. The Commission also considers requiring customer notification prior to the release of CPNI. Such proposals would be prohibitively expensive for small and regional carriers, particularly in instances where the security of CPNI has not been jeopardized. Carriers' employees are already on heightened alert for false claims for CPNI. Individual companies have various procedures to prevent unauthorized release of CPNI. Imposition of federal regulation is not necessary. Such action could, in fact, negate some of the measures already used by carriers by detracting from the creativity of local managers and diverting funds to mechanisms that may or may not improve carriers' own fraud prevention techniques. Carriers already notify customers of CPNI breaches. Decisions regarding

when and how to notify customers of CPNI access should be left to carriers.

6. Reporting

Requiring carriers to report all instances of unauthorized access to or disclosure of CPNI would impose a burden on industry not justified by the public interest. CPNI security breaches are handled best at the local level, among the carrier, customer and law enforcement. Compilation by the Commission of a record of all CPNI incidents would do nothing to improve CPNI security; it would only add unnecessarily to the obligations of carriers and FCC staff.

Carriers' annual compliance certificate is already available to the public. Requiring that it also be filed with the Commission, and that it include an explanation of actions taken against data brokers and a summary of CPNI consumer complaints, is unjustified. The Commission has no proposal for what it would do with the certifications or attached information, or how their collection would protect consumers. The proposed requirement is simply a new and duplicative reporting burden that will endure in perpetuity, will add to the costs of operation, and will disadvantage small and regional carriers with the cost of compliance.

III. Small and Regional Wireless Carriers Should Not be Burdened with New CPNI Obligations because there is Insufficient Evidence of Harm to Consumers from Misuse of CPNI

Adoption of the FCC's proposals would add unnecessarily and disproportionately to the cost of conducting business by small and regional wireless carriers. Companies of this size do not have the same administrative and financial resources as the nationwide carriers. Importantly, the proposals do not enhance the security of the CPNI of their customers. Internal practices for detection of nefarious attempts to access CPNI have proven remarkably sufficient among small and regional carriers. Such carriers do not have a history of unauthorized use or release of CPNI. Carriers serving rural areas are known for close relationships with the community and the local

customer, making the carriers all the more adept at sensing and preventing unauthorized access and use of CPNI. Enforcing upon small and regional carriers extraordinary encryption, retention, notification and reporting requirements would not enhance security; however, the proposed menu of new requirements would add significantly to the regulatory cost burdens of providing network facilities for smaller groups of subscribers.

The cost of equipment, software, maintenance, storage capacity and labor necessary to comply with the Commission's proposals would be very expensive, a fact perhaps not immediately appreciated by EPIC or by the FCC. To impose upon small and regional carriers another set of unfunded mandates to address a problem that has not been identified as significant is outside the public interest. The proposed requirements would unfairly reduce the competitive position of small and regional carriers to a degree far greater than the degree to which they would protect the interests of customers.

IV. Conclusion

RCA opposes the imposition of costly new regulatory burdens on small and regional carriers. CPNI already receives extraordinary protection from existing FCC rules and improving industry practices. The suggestions submitted by EPIC for gripping control by the FCC of all CPNI procedures are not necessary for consumer protection.

EPIC's ideas are valuable, but they are beyond the bounds of rational governmental regulation. The FCC should exercise discretion in its rulemaking, refrain from adoption of ancillary requirements, and permit industry and consumers to achieve the safeguards for CPNI that are most appropriate for the services offered and the privacy interests at stake. Industry has done a good job at tightening CPNI use and access. That progress should be rewarded with

governmental aversion to costly, new regulations.

Respectfully submitted,

RURAL CELLULAR ASSOCIATION

[filed electronically]

David L. Nace
Pamela L. Gist
Its Attorneys

LUKAS, NACE, GUTIERREZ & SACHS, CHARTERED
1650 Tysons Boulevard, Suite 1500
McLean, Virginia 22102
(703) 584-8678

April 28, 2006