

**Before the  
THE OFFICE OF MANAGEMENT AND BUDGET  
Washington, D.C. 20503**

In the Matter of	)	
	)	
Federal Communications Commission	)	OMB Control No. 3060-0715
Public Information Collection Requirement	)	
Submitted to OMB for Emergency Review	)	
And Approval	)	
	)	
Telecommunications Carriers' Use of Customer	)	CC Docket No. 96-115
Proprietary Network Information and Other	)	
Customer Information	)	

**COMMENTS OF  
THE WESTERN TELECOMMUNICATIONS ALLIANCE**

The Western Telecommunications Alliance ("WTA") submits these comments opposing various unnecessary and unduly burdensome information collection requirements adopted by the Federal Communications Commission ("FCC") in its Report and Order and Further Notice of Proposed Rulemaking (*Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Consumer Information*), CC Docket No. 96-115 and WC Docket No. 04-36, FCC 07-22, released April 2, 2007 ("CPNI Pretexting Order"), for which the FCC is presently seeking approval from the Office of Management and Budget ("OMB") under the Paperwork Reduction Act of 1995. WTA particularly opposes proposed new FCC information collection requirements: (1) in Section 64.2010 of the FCC Rules that require rural telephone companies and other small carriers to compile, maintain and safeguard files of passwords and back-up authentication materials that must be utilized before such carriers can answer heretofore routine service and billing questions from their customers; (2) in Section 64.2009(e) of the FCC Rules that require substantial annual filings with regard to customer proprietary network

information (“CPNI”) operating procedures, actions against data brokers and customer complaints; and (3) in Section 64.2011 of the FCC Rules that require the Federal Bureau of Investigation (“FBI”) and United States Secret Service (“USSS”) to be notified of all breaches of the security of CPNI files maintained by telecommunications carriers.

### **The Western Telecommunications Alliance**

The Western Telecommunications Alliance is a trade association that represents approximately 250 rural telephone companies operating west of the Mississippi River.

WTA members are generally small independent local exchange carriers (“ILECs”) serving sparsely populated rural areas. Most members serve less than 3,000 access lines overall and less than 500 access lines per exchange. Their primary service areas are comprised of sparsely populated farming and ranching regions, isolated mountain and desert communities, and Native American reservations.

### **Actual Scope of the Problem Addressed**

The CPNI Pretexting Order was adopted and issued by the FCC expressly to address the obtaining by data brokers or pretexters of unauthorized access to the CPNI of telecommunications carriers, and the placing of such CPNI on websites where it could be viewed for a price. CPNI Pretexting Order at par. 2. In most cases, the CPNI belonged to internationally, nationally or regionally prominent government officials, politicians, businessmen, journalists, entertainers and sports figures whose calling practices might be of “interest” to large numbers of website visitors. *Id.* at n. 31. In other instances, the CPNI belonged to law enforcement officials and journalists whose calling practices were likely to be of “interest” to wealthy targets they might be investigating.

The CPNI Pretexting Order indicated that the targeted CPNI abuses predominately involved unauthorized acquisition and sale of the CPNI of wireless carriers. *Id.* at notes 31, 33, 34, 35 and 36. The problem also appears to have been focused primarily in urban areas such as Chicago and Los Angeles. *Id.* at n. 31.

WTA is aware of no instances where data brokers or pretexters have obtained unauthorized access to the CPNI of the customers of its rural ILEC members and attempted to sell such CPNI on the Internet or elsewhere. WTA also has not heard of any cases of unauthorized acquisition and sale of the CPNI of customers of rural ILECs that do not belong to WTA. In other words, the problem sought to be addressed by the FCC's subject new regulations and information collection requirements has not been a rural ILEC problem, and is not likely to become a rural ILEC problem within the foreseeable future.

It is WTA's information and belief that the pretexting problem has primarily involved Cingular Wireless (now AT&T Wireless), Verizon Wireless, Sprint Nextel, T-Mobile and a handful of other large, predominately wireless, urban carriers. Most telecommunications carriers (including many urban carriers, mid-sized carriers, rural wireless carriers and rural competitive local exchange carriers as well as rural ILECs) have not been significant targets or victims of data brokers or pretexters. Nevertheless, **ALL** telecommunications carriers have been subjected to the FCC's new regulations and information collection requirements whether or not their CPNI has been acquired and sold in an unauthorized manner, or is reasonably likely to be acquired and sold in the future.

WTA believes that the vastly more effective and efficient approach is to use the criminal penalties of the recently enacted Telephone Records and Privacy Protection Act of 2006, Pub. L. No. 109-476, 120 Stat. 3568, to attack directly data brokers and pretexters who obtain

unauthorized access to calling records and other CPNI, as well as website owners and operators who acquire and attempt to sell such data. Federal resources would be much better used to investigate and prosecute specific and substantial instances of lawbreaking than to monitor the CPNI compliance programs of tens thousands of carriers that are never likely to attract the attention of a pretexter or data broker.

#### **Section 64.2010 Password and Back-Up Customer Authentication Requirements**

Section 64.2010 of the FCC Rules requires all telecommunications carriers to compile, maintain and safeguard files of passwords and back-up customer authentication materials that must be utilized before such carriers can answer heretofore routine telephone inquiries from their customers. Whereas the FCC has provided mail response and call-back options, the password and back-up authentication procedures constitute the only way for a customer to obtain a prompt resolution of a billing or service complaint if he or she is not calling from his or her "telephone number of record" (usually, the home phone).

Many WTA members that have begun to collect passwords from customers in anticipation of a December 8, 2007 or later effective date for the FCC'S new CPNI rules have encountered significant opposition and anger from their customers. Customers purely and simply do not like passwords, and do not want to have to remember and provide a password in order to ask their telephone company a billing or service question and receive an immediate answer. The FCC was well aware of this consumer dislike, *Id.* at n. 47, but proceeded to adopt comprehensive password requirements anyway.

In rural communities, password opposition and problems are far more acute than in urbanized areas. Put simply, people in rural communities associate with each other regularly at community, church, school, social, athletic and business functions and know each other

personally and by voice. If a rural ILEC customer service representative is required to obtain a password from a friend of 10-20 years before she can assist the person with a billing or service problem, she is going to encounter anger and resentment, particularly if the friend is not able to get an immediate answer because he or she cannot remember the password. For the OMB and FCC personnel reviewing this, please imagine the response that you might receive if you were to tell your relatives, friends or neighbors that you could not discuss certain matters with them over the telephone unless they first supplied a password.

As rural ILECs encounter more and more competition from wireless carriers and cable television operators, one of their primary competitive advantages has been the prompt, friendly and personalized service they provide to their customers. The proposed password and back-up customer authentication requirements place a substantial and unnecessary barrier between rural ILECs and their customers, and threaten to impair or destroy one of the superior carrier-customer environments in the telecommunications industry.

What increasingly angers rural ILECs and their customers is that the proposed password and back-up authentication requirements are wholly unnecessary in rural areas. First, there have been no problems of unauthorized acquisition and sale of rural ILEC CPNI by pretexters or bdata brokers. Second, in the unlikely event that a rural ILEC or its customers were to be targeted by a pretexter, the rural ILEC's customer service representatives can authenticate virtually all customers by their familiar voice or by a simple conversational question regarding a recent meeting or activity. It is wholly unnecessary and unduly burdensome for rural ILECs to spend thousands of hours compiling, organizing, administering and safeguarding passwords and back-

up authentication question databases<sup>1</sup> when the only significant impact of such efforts will be to anger their customers.

WTA requests OMB to reject the FCC's proposed Section 64.2010 password and back-up customer authentication rules as unnecessary and unduly burdensome information collection requirements. In the alternative, WTA recommends that OMB ask the FCC to limit the applicability of these Section 64.2010 requirements to telecommunications carriers that are found actually to have permitted data brokers and pretexters to access the CPNI of their customers in an unauthorized manner. In other words, these burdensome requirements should be imposed only where necessary to deal with carriers that have proven to be unable to protect the CPNI entrusted to them.

#### **Section 64.2009(e) Annual CPNI Compliance Certifications**

Section 64.2009(e) of the FCC Rules requires the filing of annual CPNI compliance certifications regarding a carrier's CPNI procedures, actions against data brokers and customer complaints.

This annual filing is a labor-intensive undertaking for small rural ILECs. Annual CPNI training can take at least eight-to-twenty hours for each employee than handles CPNI. Compilation and review of the statement of CPNI operating procedures attached to the annual certification can take twenty-to-fifty or more man-hours of management and consultant time. WTA members find this information gathering and paperwork unnecessary and unduly burdensome because they have not been subject to pretexter attacks and have not had their CPNI taken and sold in an unauthorized manner.

---

<sup>1</sup> WTA estimates that it will initially take at least one to two hours per customer for a rural ILEC to obtain a password from each customer and to set up a secure customer password database. Thereafter, additional time will be needed periodically to monitor, test and update the database, as well as to request passwords and check them against the database during customer telephone calls.

WTA members are willing to safeguard their CPNI in a reasonable and effective manner. However, until such time as the FCC determines that pretexter attacks and the unauthorized disclosure and sale of CPNI is an actual problem in rural ILEC service areas, the Section 64.2009(e) annual certification requirement should not be applied to rural ILECs.

#### **Section 64.2011 Notifications to FBI and Secret Service**

Section 64.2011 of the FCC Rules requires notification of the FBI and USSS of all breaches of the security of CPNI files maintained by telecommunications carriers.

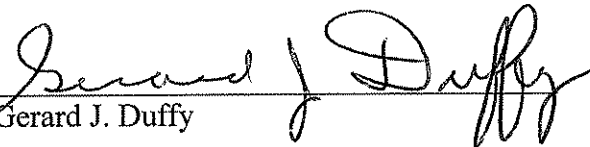
WTA members do not object to this requirement as carriers. However, as United States citizens, they are concerned that the breadth of the requirement to report “all breaches” will overwhelm the FBI and USSS with trivial investigations and paperwork that will impair their ability to execute critical national security and law enforcement responsibilities. For example, it is likely that many “breaches” of CPNI security are initiated by spouses and their friends and agents to determine whether the other spouse is cheating. Do the OMB and the FCC really want FBI and USSS agents urgently needed for anti-terrorist and executive protection duties to be wasting hours and hours of their valuable time investigating attempts by angry spouses to get the phone records of their existing or estranged partners?

#### **Conclusion**

WTA reiterates that the unauthorized CPNI acquisition and sale issues addressed in the FCC’s CPNI Pretexting Order are predominately wireless carrier and urban issues. Similar problems have not arisen with rural ILECs or in rural ILEC service areas. In particular, the FCC’s proposed new Section 64.2010 password and back-up customer authentication requirements are not only unnecessary and unduly burdensome in rural ILEC service areas, but also are likely to significantly harm carrier-customer relationships and decrease consumer

satisfaction. The proposed new Section 64.2010 requirements should be eliminated. In the alternative, such requirements, as well as the Section 64.2009(e) annual CPNI compliance certification filing requirement, should be imposed only upon carriers that have actually failed to protect CPNI from unauthorized acquisition and sale by data brokers or pretexters.

Respectfully submitted,  
**WESTERN TELECOMMUNICATIONS ALLIANCE**

By   
Gerard J. Duffy

Its Attorney

Blooston, Mordkofsky, Dickens,  
Duffy & Prendergast, L.L.P.  
2120 L Street, NW (Suite 300)  
Washington, DC 20037  
Phone: (202) 659-0830  
Facsimile: (202) 828-5568  
Email: [gjd@bloostonlaw.com](mailto:gjd@bloostonlaw.com)

Dated: November 21, 2007