



# Commnet Wireless, LLC

---

February 27, 2009

Ms. Marlene H. Dortch  
Office of the Secretary  
Federal Communications Commission  
445 12<sup>th</sup> Street, S.W., Suite TW-A325  
Washington, D.C. 20554

Re: Annual 64.2009(e) CPNI Certification for 2008 ("Amended")  
Form 499 Filer ID<sup>1</sup>  
**EB Docket No. 06-36**

Dear Ms. Dortch:

Pursuant to §64.2009(e) of the Commission's rules, Commnet Wireless, LLC, on behalf of itself and its various licensee subsidiaries and affiliates identified in footnote 1 *infra* (collectively, "Commnet"), hereby certifies that the company has established operating procedures that are adequate to ensure compliance with the rules set forth in Subpart U of Part 64 of the commission's Rules.

Commnet, a wireless carrier holding cellular and PCS licenses, operates 100% as a "carriers' carrier", selling its services only on a wholesale basis to other cellular and PCS licensees. Commnet has no retail customers and no sales or marketing department. Commnet does not generate or send out invoices – rather, Commnet receives its revenues through the general settlement processes of the carrier roaming clearinghouses. Thus, Commnet possesses no CPNI, as that term is defined in §222 of the Communications Act of 1934, as amended. Therefore, there is no CPNI to protect. Since Commnet possesses no CPNI, by definition, there is nothing more Commnet could say respecting company operating procedures to protect CPNI. Nevertheless, since Commnet is planning to initiate retail operations later in 2009, attached is the written policy explaining the company's procedures that ensure the company's compliance with the requirements of the CPNI Rules, if and when the company ever comes into possession of any CPNI. The company will distribute a copy of this written policy to all personnel, and shall train all personnel to maintain customer records as proprietary information and to not share such information with any outside parties, prior to initiating any retail operations.

Commnet did not take any actions against data brokers in the past year. Also, having no customers, Commnet did not receive any customer complaints in the past year concerning the unauthorized release of CPNI.

I, the undersigned, hereby certify under penalty of perjury that I am an officer of Commnet and am responsible for the preparation of this certificate. I further certify to the truth and accuracy of the information contained in this certificate, that I have personal knowledge of Commnet's operating procedures, and that Commnet has established operating procedures adequate to ensure compliance with the FCC's CPNI rules set forth in §§64.2001 *et seq.*

Louis J. Tomasetti  
President & CEO

cc: Best Copy and Printing, Inc. (1 copy)

---

<sup>1</sup> Each of Commnet's subsidiaries and affiliates files its own Form 499A and, thus, each has been assigned its own Form 499 Filer ID number, which are as follows: Commnet of Arizona – No. 823492; Elbert County Wireless – No. 822200; Excomm – No. 822196; Commnet of Florida – No. 822208; Commnet Four Corners – No. 823490; Gila County Wireless – No. 826547; Commnet Midwest – No. 827014; and Mora Valley Wireless – No. 827015. All other Commnet subsidiaries are also covered by this letter; however, the other subsidiaries had not initiated any commercial operations (wholesale or retail), as of December 31, 2008.

## CUSTOMER INFORMATION POLICY

**To protect the proprietary and private information about our customers, Commnet Wireless, LLC, for itself and all subsidiaries and affiliates, establishes this company policy regarding customer information:**

1. All of the company's proprietary data bases, including that containing customer information, are password protected, and access to same is limited to authorized personnel only. Distribution of the password is limited to those authorized personnel. The password will be changed routinely, and whenever an employee with access to such data bases leaves the company.
2. No customer information in any form is to be removed from the company's offices by employees or others. This includes computer printouts, handwritten information or notes, copies of files or documents in any electronic form, and verbal transmission of customer information to persons who are not direct employees of the company.
3. Employees are to closely guard customer lists, contact information, telephone numbers, mobile code lists and all other customer information, both proprietary and public, to prevent any information from being removed from our offices by non-employees either accidentally or intentionally.
4. The notes a salesperson may make about a customer, number of mobiles in use and mobile numbers to assist in a sale must be returned to the company's office and re-filed or shredded. If, for example, a salesperson is making a sales call to Customer A to discuss adding more mobiles for Customer A, the salesperson may need to take information on the number of mobile units already in service at Customer A. This information is to be shared only with the customer who is using those mobile units. At the completion of the sales call, the information is to be returned to the office and re-filed or shredded.
5. Internal documents, notes made when customers call in, and anything containing customer names and telephone numbers must be shredded at the end of the business day.
6. Each new customer is required to select a personal password and provide the company with certain non-public information that only the customer knows, such as a favorite pet's name, etc., which password and information is to be used for identification purposes. Upon contact with a customer, you must request that the customer confirm his/her identity by providing you with his/her pre-existing password and pre-selected information before discussing any matter with the customer
7. Customer information is never to be used or disclosed to anyone, except as follows:
  - (a) to market the company's service offerings to which the customer already subscribes;
  - (b) to market the company's CPE, information services, and adjunct-to-basic services;
  - (c) for purposes of conducting health effects research;

- (d) to protect the company's own rights and property, and to protect the rights of other carriers or other users of services from fraudulent, abusive or unlawful use;
  - (e) to disclose all location information in emergency situations, as provided for under §§222(d)(4) & (f) of the Communications Act of 1934, as amended;
  - (f) to comply with the company's obligations to provide certain customer information when lawfully requested by law enforcement authorities pursuant to the Communications Assistance for Law Enforcement Act ("CALEA"); and
  - (g) to resolve specific customer questions about the customer's own account, arising in the course of a telephone conversation between that customer and company's service representative, and then only after orally obtaining from the customer a limited, one-time authorization to use the customer's information for the duration of that phone call.
8. Disconnected or inactive customer files are to be retained for no more than 3 years, and then shredded. Disconnected or inactive customer files are never to be placed in the trash unshredded. Customer database printouts are to be shredded when replaced by newer printouts.
9. Appropriate disciplinary action will be taken for any violations of this policy.