

February 27, 2009

Marlene H. Dortch  
Office of the Secretary  
Federal Communications Commission  
445 12<sup>th</sup> Street, SW, Suite TW-A325  
Washington, DC 20554

RE: EB Docket No. 06-36

Dear Ms. Dortch;

Enclosed on behalf of Knology Total Communications (f.k.a. Graceba Total Communications, Inc.) - Form 499 Filer ID 802146 please find the Customer Proprietary Network Information (CPNI) certification and statement of procedures.

Should you require additional information, please do not hesitate to contact me. I can be reached at (706) 645-3966 or via email at [bruce.schoonover@knology.com](mailto:bruce.schoonover@knology.com)

Sincerely,



Bruce Schoonover, Jr.  
Director – Regulatory Affairs  
Knology, Inc.

Enclosures

cc: Best Copy and Printing, Inc.

**Certificate**  
**EB Docket No. 06-36**

Annual 64.2009(e) CPNI Certification for 2008

Date Filed: February 27, 2009

Name of Company covered by this certification: Knology Total Communications, Inc.  
(f.k.a. Graceba Total Communications, Inc.)

Form 499 Filer ID: 802146

Name of Signatory: Chad Wachter

Title of Signatory: VP, General Counsel and Secretary

I, Chad Wachter, certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to insure compliance with the Commission's CPNI rules.

Attached to this certification is an accompanying statement explaining how the company's procedures ensure that the company is in compliance with the requirements set forth in section 64.2001 et seq. of the Commission's rules. The company has not taken any actions (proceedings instituted or petitions filed by the company at either state commissions, the court system, or at the Commission) against data brokers in 2008. Customer service and sales personnel are trained on the need to maintain the confidentiality of CPNI and to be alert to attempts by unauthorized persons to access CPNI. All company personnel with access to CPNI records know that only properly identified and authenticated customers can have access to his/her CPNI. Any questionable activity with regard to the access to or the use or distribution of CPNI is immediately reported to the legal department and the Compliance Officer for review. The company has not detected any attempts by pretexters or other unauthorized persons to access CPNI.

The company has not received any customer complaints in the past year concerning the unauthorized release of CPNI.

Signed \_\_\_\_\_

**Statement of Company Procedures**  
**EB Docket No. 06-36**

The following facts support the certification:

1. The company uses the opt-out procedure to determine whether a customer consents to the use of its CPNI for internal marketing of communications related services to the customer. Every two years the company notifies all customers of the company's duty to protect CPNI and the customers' right to have that CPNI protected and not used for the purpose of marketing telecommunications related services to them. The customers are also informed of the opportunity and method to notify the company at any time to opt-out of the use the customers' CPNI for those marketing purposes. The notice explains CPNI, the marketing purposes for which the company would want to use CPNI, and the 24/7/365 method for opting-out. When the customer contacts the company to opt-out, the appropriate notations made to the company's records to ensure the CPNI is not inappropriately used. The last two-year notice was mailed in November 2008 and the next notification will occur on or before that date in 2010. Approximately 10 customers have opted-out of using their CPNI for marketing purposes. Sales and customer care personnel know that the failure to opt-out is not effective until 33 days after the date of the opt-out notification.
2. All customer care and sales personnel are trained by their respective supervisors on the policies and procedures of the company including those that are applicable to CPNI protection and use. The customer care group is trained frequently throughout the year on CPNI and other privacy concerns. The company does have a PIN protection system in place to limit access to an account to the customer of record. If for whatever reason the account is not PIN protected, personnel are trained and monitored on customer authentication using information other than readily available biographical customer information.
3. The company did not initiate a password authentication for customer access to his/her CPNI in 2008.
4. The company did not conduct any sales and marketing campaigns in 2008 using CPNI. The company did not need or seek any opt-in consents. The company does not use a joint venture partner or third parties for the purpose of marketing communications related services to customers.
5. The company did not release any CPNI to third parties for marketing or any other purposes in 2008.
6. The supervisors of the company's sales and customer care operations monitor data security on a daily basis. No use of CPNI is authorized without approval of these supervisors and the Legal Department/Compliance Officer. Release of CPNI to law enforcement or through other legal process must be reviewed and approved by the Legal

Department. All marketing information and materials are reviewed by the Legal Department/Compliance Officer before use or deployment. The unauthorized access to or use or disclosure of CPNI is punishable under the company's Employee Guidebook by disciplinary actions up to and including termination of employment.