

AGNES PENNINGTON
9921 CARMEL MTN. RD.
SAN DIEGO, CA 92129-2813
(P) 858-538-0403
(F) 858-335-4355

VIA ELECTRONIC FILING

Marlene H. Dortch, Office of the Secretary
Federal Communications Commission
445 12th St. S.W.
Suite TW-A325
Washington, D.C. 20554

Re: Annual 47 C.F.R. 64.2009 (c) Certification for 2008
EB Docket No. 06-36
Agnes Pennington
FRN: 0004616959

I, Agnes Pennington, hereby certify that I am an officer of the company named above, and acting as agent of the company, that I have personal knowledge that the company established operating procedures effective during the calendar year of 2008 that are adequate to ensure compliance with the CPNI rules set forth in 47 C.F.R. 64.2001-2011 of the rules of the Federal Communications Commission.

Attached to this certification is an accompanying statement which explains how the company's procedures ensure that the company is in compliance with the requirements set forth in 47 C.F.R. 64-2001 et seq. of the Federal Communications Commission's rules and also explains any action taken regarding tactics against data brokers during the past year and reports information known to the company regarding pretexters may be using to attempt access to CPNI and summarizes any customer complaints received in the past year concerning the unauthorized release of CPNI.

Agnes Pennington
Consultant
February 22, 2009

Agnes Pennington
CPNI Certification
FRN: 0004616959

STATEMENT

I, Agnes Pennington, (“Carrier”) have established operating procedures that ensure compliance with the Federal Communications Commission (“Commission”) regulations regarding the protection of customer proprietary network information (“CPNI”).

- Carrier has adopted a manual and keeps it updated with the Commissions CPNI rule revisions and has designated a CPNI compliance officer to oversee CPNI training and implementation.
- Carrier continually educated and trains its employees regarding the appropriate use of CPNI. Carrier has established disciplinary procedures should an employee violate the CPNI procedures established by Carrier.
- Carrier has implemented a system whereby the status of a customer’s CPNI approval can be determined prior to use of CPNI.
- Carrier maintains a record of its and its affiliates’ sales and marketing campaigns that use its customers’ CPNI. Carrier also maintains a record of any and all instances where CPNI was disclosed or provided to third parties, or where third parties were allowed access to CPNI. The record includes description of each campaign, the specific CPNI that was used in the campaign, and what products and services were offered as part of the campaign.
- Carrier has established a supervisory review process regarding compliance with the CPNI rules with respect to outbound marketing situations and maintains records of carrier compliance for a minimum period on one year. Specifically, Carrier’s sales personnel obtain supervisory approval of any proposed outbound marketing request for customer approval regarding its CPNI, and a process ensures that opt-out elections are recorded and followed.

Carrier has established procedures to notify law enforcement and customer(s) of unauthorized disclosure of CPNI in accordance with the Commission timelines.

Carrier took the following actions against data brokers in 2008, including proceedings instituted or petitions filed by Carrier at a state commission, in the court system, or at the Federal Communications Commission: **None**

Agnes Pennington
CPNI Certification
FRN: 0004616959

- The following is information Carrier has with respect to the processes pretexters are using to attempt to access CPNI, and (if any) what steps carriers are taking to protect CPNI; **Carrier has determined that no pretexter has attempted to access CPNI Carrier's system.**

The following is a summary of all customer complaints received in 2008 regarding the unauthorized release of CPNI:

- Number of customer complaints Carrier received in 2008 related to unauthorized access to CPNI or unauthorized disclosure of CPNI: **None**
- Category of complaint:
 - **0** Number of instances of improper access by employees
 - **0** Number of instances of improper disclosure to individuals not authorized to receive the information
 - **0** Number of instances of improper access to online information by individuals not authorized to view the information
 - **0** Number of other instances of improper access or disclosure
- Description of instances of improper access or disclosure: **None**