Talk of the Thumb!
Thumb Cellular
A Subsidiary of Agri-Valley Communications, Inc.

EB Docket No. 06-36

February 18, 2009

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

RE: Annual 64.2009(e) CPNI Certification for 2008
Filing Period: March 1, 2009
Name of company covered by this certification: Thumb Cellular, LLC
Form 499 Filer ID: 814905
Name of signatory: Edwin H. Eichler
Title of signatory: President, Parent Company

Dear Secretary Dortch,

In accordance with 47 CFR 64.2009(e), please find attached the Company's Annual Compliance Certificate for the previous calendar year, 2008. The Compliance Certificate includes the Company's:

- Statement explaining how its operating procedures ensure compliance with 47 CFR, Part 64, Subpart U;
- An explanation of any actions taken against data brokers; and
- A summary of all customer complaints received in the past year concerning the unauthorized release of customer proprietary network information (CPNI).

If you have any questions regarding this filing, please direct them to the undersigned.

Sincerely,

Edwin H. Eichler
President, Parent Company

Enclosure

cc: Federal Communications Commission, Enforcement Bureau, Telecommunications Consumers Division, 445 12th Street SW, Washington, DC 20554 (2 courtesy copies)
Best Copy and Printing, Inc., **FCC@BCPIWEB.COM**

P.O. Box 650 • Pigeon, Michigan 48755 • (989) 453-4333 • Fax: (989) 453-4363 • www.thumbcellular.com

CERTIFICATE OF COMPLIANCE WITH PROTECTION OF CUSTOMER PROPRIETARY NETWORK INFORMATION RULES

Including:

Statement Explaining How Operating Procedures Ensure Regulatory Compliance

Explanation of Any Actions Against Data Brokers, and

Summary of all Customer Complaints Received

Edwin H. Eichler signs this Certificate of Compliance in accordance with § 222 of the Telecommunications Act of 1996, as amended, 47 USC 222, and 47 CFR 64.2009, on behalf of Thumb Cellular LLC (Company), related to the previous calendar year, 2008.

This Certificate of Compliance addresses the requirement of 47 CFR 64.2009 that the Company provide:

- A "statement accompanying the certificate" to explain how its operating procedures ensure compliance with 47 CFR, Part 64, Subpart U;
- An explanation of any actions taken against data brokers; and
- A summary of all customer complaints received in the past year concerning the unauthorized release of customer proprietary network information (CPNI).

On Behalf Of The Company, I Certify As Follows:

1. I am the President of the Company, and therefore an officer of the Company. My business address is 7585 West pigeon Road, Pigeon MI, 48755 The Company's Form 499 Filer ID is 804396.

2. I have personal knowledge of the facts stated in this Certificate of Compliance. I am responsible for overseeing compliance with the Federal Communications Commission's (FCC) rules relating to CPNI.

Statement Explaining How Operating Procedures Ensure Regulatory Compliance

3. I have personal knowledge that the Company has established operating procedures that are adequate to ensure compliance with the FCC's regulations governing CPNI, including those adopted on March 13, 2007 in CC Docket No. 96-115.

4. The Company ensures that it is in compliance with the FCC's CPNI regulations. The Company trains its personnel regarding when they are authorized to use CPNI, when they are not authorized to use CPNI, and how to safeguard CPNI. The Company maintains a CPNI Compliance Manual in its offices for purposes of training of new and current employees, and as a reference guide for all CPNI issues. Our CPNI Compliance Manual is updated to account for changes in law, including the FCC's most recent changes to its regulations governing CPNI, adopted on March 13, 2007 in CC

Docket No. 96-115. The CPNI Manual contains key all essential information and forms to ensure the Company's compliance with CPNI regulations.

5. The Company has established a system by which the status of a Customer's approval for use of CPNI, as defined in 47 USC 222(h)(1), can be clearly established prior to the use of CPNI. The Company relies on the involvement of its high-level management to ensure that no use of CPNI is made until a full review of applicable law has occurred.

6. Company personnel make no decisions regarding CPNI without first consulting with management.

7. The Company has an express disciplinary process in place for personnel who make unauthorized use of CPNI.

8. The Company's policy is to maintain records of its own sales and marketing campaigns that use CPNI. The Company likewise maintains records of its affiliates' sales and marketing campaigns that use CPNI. The Company also maintains records of all instances where CPNI was disclosed or provided to third parties, or where third parties were allowed access to CPNI. These records include a description of each campaign, the specific CPNI that was used in the campaign, and the products and services that were offered as a part of the campaign. The Company maintains these records in its offices for a minimum of one year.

9. In deciding whether the contemplated use of the CPNI is proper, management consults one or more of the following: the Company's own compliance manual, the applicable FCC regulations, and, if necessary, legal counsel. The Company's sales personnel must obtain supervisory approval regarding any proposed use of CPNI.

10. Further, management oversees the use of opt-in, opt-out, or any other approval requirements, or notice requirements (such as notification to the Customer of the right to restrict use of, disclosure of, and access to CPNI), contained in the FCC's regulations. Management also reviews all notices required by the FCC regulations for compliance therewith. Before soliciting for approval of the use of a Customer's CPNI, the Company will notify the Customer of his or her right to restrict use of, disclosure of, and access to, his or her CPNI.

11. The Company maintains records of Customer approval and disapproval for use of CPNI in a readily-available location that is consulted on an as-needed basis.

12. The Company complies with all FCC requirements for the safeguarding of CPNI, including use of passwords and authentication methods, and the prevention of access to CPNI (and Call Detail Information in particular) by data brokers or "pre-texters."

13. The Company, on an ongoing basis, reviews changes in law affecting CPNI, and updates and trains company personnel accordingly.

Explanation of Actions Against Data Brokers

14. The Company has encountered one circumstance requiring it to take any action against a data broker during the year to which this Certificate pertains. *[See Attachment A)*

Summary of all Customer Complaints Received

15. The following is a summary of all customer complaints received in the past year concerning the unauthorized release of CPNI: *[See Attachment A)*

16. As discussed more fully in Attachment A below there has been one case of in which a pretexter/phisher attempted to access CPNI, however, no breach occurred.

Date: February 18, 2009 Edwin H. Eichler

ATTACHMENT A

Customer Account or Mobile No.	General Nature of Complaint	Date Complaint Received	Employees Who Investi-gated	Information Revealed in Investigation	Date The Investi-gation Ended	Result of Company's Investigation
Phone number and subscriber name will be made available to the FCC upon request	Customer raised concern over potential improper disclosure to an individual not authorized to receive the info.	9/17/08	Brenda Ahearn; Catherine Pavley	Discovered two phishing attempts by an apparent sales representative of T-Mobile: - Customer's daughter went to T-Mobile to port her phone as she was moving out of the area. An apparent T-Mobile sales rep called Thumb Cellular's customer service and pretended to be the brother of that female (i.e., the son of a Thumb Cellular customer) seeking customer information. Since neither the brother nor daughter was an authorized user, no information was given. -- Later that same day, the same T-Mobile rep appeared to ask that same female (customer's daughter) to get the customer's social security number, date of birth, and drivers license number to gain access to the account. Again, no information was disclosed to T-Mobile rep or the female.	9/22/08	No breach. But since there was an apparent phishing attempt by a T-Mobile sales rep, the matter was reported to the FBI/Secret Service.
Phone number and subscriber name will be made available to the FCC upon request	Concern over potential improper disclosure to an individual not authorized to receive the info.	9/22/08	Kathy Lecznar; Helen St. Louis; Megan Smith	Customer called Thumb Cellular office inquiring if he was still under contract. When he was advised that he was since his daughter had recently signed a contract, he claimed his daughter was not authorized to do so. However, account notes indicate that, about two months prior to the customer's present inquiry, he advised that his daughter was coming to a Thumb Cellular office to make changes to the account and that he was authorizing her to do so.	9/22/08	No breach.