

LUKAS, NACE, GUTIERREZ & SACHS, LLP

8300 GREENSBORO DRIVE, SUITE 1200
MCLEAN, VIRGINIA 22102
703 584 8678 • 703 584 8696 FAX

WWW.FCCLAW.COM

RUSSELL D. LUKAS
DAVID L. NACE
THOMAS GUTIERREZ*
ELIZABETH R. SACHS*
DAVID A. LAFURIA
PAMELA L. GIST
TODD SLAMOWITZ*
BROOKS E. HARLOW*
TODD B. LANTOR*
STEVEN M. CHERNOFF*
KATHERINE PATSAS NEVITT*

CONSULTING ENGINEERS
ALI KUZEHKANANI
LEILA REZANAVAZ
—
OF COUNSEL
GEORGE L. LYON, JR.
LEONARD S. KOLSKY*
JOHN CIMKO*
J. K. HAGE III*
JOHN J. MCAVOY*
HON. GERALD S. MCGOWAN*
TAMARA DAVIS BROWN*
JEFFREY A. MITCHELL*
ROBERT S. KOPPEL*
MARC A. PAUL*

*NOT ADMITTED IN VA

Writer's Direct Dial
(703) 584-8665
pgist@fcclaw.com

February 22, 2012

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

Re: EB Docket No. 06-36
Annual 47 C.F.R. § 64.2009(e) CPNI Certification for 2011

Bluegrass Cellular, Inc.
Kentucky RSA #3 Cellular General Partnership
Kentucky RSA 4 Cellular General Partnership
Cumberland Cellular Partnership
Bluegrass Wireless LLC

Dear Ms. Dortch:

On behalf of Bluegrass Cellular, Inc. and its affiliates, and pursuant to Section 64.2009(e) of FCC rules, submitted herewith is the carriers' joint CPNI certification with accompanying statement covering calendar year 2011.

Should any questions arise regarding this submission, please contact the undersigned.

Very truly yours,



Pamela L. Gist

Enclosure

cc: Best Copy and Printing, Inc.

Annual 47 C.F.R. § 64.2009(e) CPNI Certification
EB Docket No. 06-36

Annual 64.2009(e) CPNI Certification for 2011
Date filed: February 22, 2012

Name of companies covered by this certification:

Bluegrass Cellular, Inc.

For and on behalf of

Kentucky RSA #3 Cellular General Partnership
499 Filer ID 802218

Kentucky RSA #4 Cellular General Partnership
499 Filer ID 802215

Cumberland Cellular Partnership
499 Filer ID 802221

Bluegrass Wireless LLC
499 Filer ID 825310

Address: P.O. Box 5012
Elizabethtown, Kentucky 42702

Name of signing officer: Ronald R. Smith
Title of signatory: President

CERTIFICATION

I, Ronald R. Smith, hereby certify that I am an officer of the companies named above, and acting as an agent of the companies, that I have personal knowledge that the companies have established operating procedures that are adequate to ensure compliance with the Customer Proprietary Network Information rules set forth in 47 C.F.R. §§ 64.2001 *et seq.* of the rules of the Federal Communications Commission.

Attached to this certification is an accompanying statement which (i) explains how the companies' procedures ensure that the companies are in compliance with the requirements set forth in 47 C.F.R. §§ 64.2001 *et seq.* of the Commission's rules, (ii) explains any action taken against data brokers during the past year, (iii) reports information known to the companies regarding tactics pretexters may be using to attempt access to CPNI, and (iv) summarizes any customer complaints received in the past year concerning the unauthorized release of CPNI.



Name: Ronald R. Smith

Title: President

Date: 2/22/12

Company Names (Collectively referred to as “Carrier”):

Bluegrass Cellular, Inc.

For and on behalf of

Kentucky RSA #3 Cellular General Partnership

Kentucky RSA #4 Cellular General Partnership

Cumberland Cellular Partnership

Bluegrass Wireless LLC

STATEMENT

Carrier has established operating procedures that ensure compliance with the Federal Communication Commission (“Commission”) regulations regarding the protection of customer proprietary network information (“CPNI”).

- Carrier has adopted a manual and keeps it updated with FCC CPNI rule revisions, and has designated a CPNI compliance officer to oversee CPNI training and implementation.
- Carrier continually educates 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 the 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 a description of each campaign, the specific CPNI that was used in the campaign, and what products and services were offered as a 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 of 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 implemented procedures to properly authenticate customers prior to disclosing CPNI over the telephone, at Carrier’s retail locations or otherwise and in connection with these procedures, Carrier has established a system of passwords and back-up authentication methods which complies with the requirements of applicable Commission rules.

- Carrier has established procedures to ensure that customers will be immediately notified of account changes including changes to passwords, back-up means of authentication for lost or forgotten passwords, or address of record.
- Carrier has established procedures to notify law enforcement and customer(s) of unauthorized disclosure of CPNI in accordance with FCC timelines.
- Carrier took the following actions against data brokers in 2011, including proceedings instituted or petitions filed by Carrier at a state commission, in the court system, or at the Federal Communications Commission:
 - No instances of CPNI violations stemming from data brokers, no action taken
- 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:
 - Call Center: Persons calling stating that they are the account holder when they are not – Verification of personal information prior to discussing the account information is used to protect CPNI. Detail call records are only mailed to the account billing address (never faxed or sent to another address).
 - Retail Location - Persons stating that they are the account holder when they are not – Verification of picture id prior to discussing any account information or release of bills or call records.
- The following is a summary of all customer complaints received in 2011 regarding the unauthorized release of CPNI:
 - Number of customer complaints Carrier received in 2011 related to unauthorized access to CPNI, or unauthorized disclosure of CPNI: 10

Category of complaint:

 - 5 Number of instances of improper access by employees
 - 5 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
 - Summary of customer complaints received in 2011 concerning the unauthorized release of CPNI:

- 2/4/11: Customer alleged that his account and call detail was being assessed by our employee who is his ex-wife. Upon investigation, we discovered our employee had not accessed this account or call detail data, a CPNI violation did not occur.
- 2/7/11: Customer alleged that our employee released account information to another customer. Upon investigation, this employee had not accessed the customer's account information, a CPNI violation did not occur.
- 3/1/11: Customer alleged that our employee was able to convey text message verbiage to the customer's ex-girlfriend. Our employee has no access to this data, a CPNI violation did not occur.
- 4/6/11: Customer alleged that his account and call information is being viewed by our employee. Upon investigation, it was determined that our employee did not access this customer's account information or call records, a CPNI violation did not occur.
- 4/18/11: Customer alleged that an employee was sharing information with other customers about the verbiage from a text message. Our employee had no access to this data, a CPNI violation did not occur.
- 5/9/11: Customer alleged that an employee accessed her account without permission. Upon investigation, the employee did not access the account, a CPNI violation did not occur.
- 5/23/11: Customer alleged that her account is being accessed by our employee without permission or business need. Upon investigation, a CPNI violation did occur and employment was discontinued.
- 7/22/11: Customer alleged that her account is being accessed by multiple locations/employees and that her information is being released to her sister. Upon investigation, it was determined that no violation took place, a CPNI violation did not occur.
- 8/8/11: Customer states that she has been receiving calls from a stranger alleging that he is obtaining information from her account. Upon investigation, the customer's account was not accessed, a CPNI violation did not occur.
- 11/1/11: Customer alleged that an ex-girlfriend was obtaining account information via on-line chat with carriers' employees. Upon investigation, employees did not disclose this customer's information, a CPNI violation did not occur.