

EAST KENTUCKY NETWORK
101 TECHNOLOGY TRAIL
IVEL, KY 41642
PHONE: (606) 874-7550
FAX: (606) 874-7551
EMAIL: INFO@EKN.COM
WEBSITE: WWW.EKN.COM



February 19, 2015

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

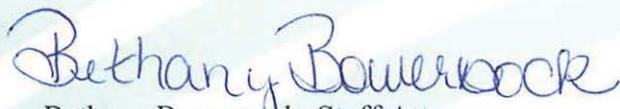
Re: EB Docket No. 06-36
Annual 47 C.F.R. 64.2009(e) CPNI Certification for 2014
East Kentucky Network, LLC d/b/a Appalachian Wireless

Dear Ms. Dortch:

On behalf of East Kentucky Network, LLC d/b/a Appalachian Wireless, and pursuant to Section 64.2009(e) of FCC rules, submitted herewith is the carrier's CPNI certification with accompanying statement covering the calendar year 2014.

If you have any questions regarding this submission, please feel free to contact me at your convenience.

Very Truly Yours,


Bethany Bowersock, Staff Attorney

Enclosure

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

Annual 64.2009 (e) CPNI Certification covering the calendar year 2014

Date Filed: February 19, 2015

Company Name: East Kentucky Network, LLC d/b/a Appalachian Wireless
101 Technology Trail
Ivel, KY 41642

Form 499 Filer ID: 802104

Name of signing officer: W.A. Gillum

Title of Signatory: Chief Executive Officer

CERTIFICATION

I, W.A. Gillum, hereby 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 ensure compliance with the Customer Proprietary Network Information (“CPNI”) 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 explaining how the company’s procedures ensure that the company is in compliance with the requirements (including those mandating the adoption of CPNI procedures, training, recordkeeping, and supervisory review) set forth in section 64.2001 *et seq.* of the Federal Communications Commission’s rules.

The company has not taken actions (i.e. proceedings instituted or petitions filed by a company at either state commissions, the court system, or at the Federal Communications Commission against data brokers) against data brokers in the past year.

The company received two (2) customer complaints in the calendar year 2014 concerning the unauthorized release of CPNI.

The company represents and warrants that the above certification is consistent with 47 C.F.R. 1.17, which requires the truthful and accurate statements to the Federal Communications Commission. The company also acknowledges that false statements and misrepresentations to the Federal Communications Commission are punishable under Title 18 of the U.S. Code and may subject it to enforcement action.



Name: W.A. Gillum

Title: CEO/General Manager

Date: February 19, 2015

Attachment: Accompanying statement explaining CPNI procedures
Summary of customer complaints

Company Name ("Carrier"): East Kentucky Network, LLC d/b/a Appalachian Wireless

STATEMENT

East Kentucky Network, LLC d/b/a Appalachian Wireless ("Carrier") has established operating procedures that ensure compliance with the Federal Communications Commission ("Commission") regulations regarding the protection of Customer Proprietary Network Information ("CPNI").

- Carrier has designated a CPNI compliance officer to oversee CPNI training and implementation.
- Carrier has a system implemented whereby the status of a customer's CPNI approval can be determined prior to the use of CPNI.
- 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.
- Carrier does not use its customer's CPNI in its or its affiliates' sales and marketing campaigns. Carrier does not conduct outbound marketing to its customers. Carrier does not provide an opt-in election to its customers; controls are established to automatically designate all customers as selecting an opt-out election.
- Carrier has procedures implemented to properly authenticate customers prior to disclosing CPNI over the telephone, at Carrier's retail locations or otherwise. Carrier has established a password system and back-up authentication methods for all customers and accounts, which complies with the requirements of applicable Commission rules.
- Carrier has procedures established to ensure that customers will be immediately notified of account changes including changes to passwords or address of record, as well as, a back up means of authentication for lost or forgotten passwords.
- Carrier has procedures established to notify law enforcement and customer(s) of unauthorized disclosure of CPNI, in accordance with Commission timelines.
- Carrier took no actions against data brokers in the calendar year 2014, including proceedings instituted or petitions filed by Carrier at a state commission, in the court system, or at the Commission.
- Carrier has found that pretexters are continuing their attempts to access CPNI through telephone calls and customer impersonation. Carrier's utilization of a passcode/pin-code system to properly authenticate customers, plus additional verification procedures, protects CPNI.
- The following is a summary of all customer complaints received in the calendar year 2014, regarding the unauthorized release of CPNI:

* Number of customer complaints Carrier received in the calendar year 2014, related to unauthorized access to CPNI or unauthorized disclosure of CPNI: 2

* Category of Complaint:

0 Number of instances of improper access by employees.

2 Number of instances of improper disclosure to individuals not authorized to receive the information.

1) A customer's account was compromised when an unauthorized individual, who was her estranged husband, called a customer service representative for Carrier and provided customer's password. Unauthorized individual then requested that the e-mail address associated with the account be changed to his personal e-mail account. Unauthorized individual further had call detail information forwarded to this new e-mail address, without authorization from Customer. Carrier does not have information relating to how the unauthorized individual obtained the customer's password. Carrier handled the violation in accordance with written CPNI policies and procedures by placing the employee on a Performance Improvement Plan, which included additional CPNI training.

2) A customer's account was compromised when the brother of the account holder went into a retail sales location and informed the retail sales associate that he had a telephone on his brother's account and would like to pay his portion of the bill. The sales associate provided the brother with amounts from the billing statement, despite the fact that he was not an authorized user. The retail sales associate in question resigned from employment before carrier learned of this improper disclosure, therefore, no further action was taken.

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.