

**Annual 47 C.F.R. § 64.2009(e) CPNI Certification**  
**EB Docket 06-36**

Annual 64.2009(e) CPNI Certification for 2018 covering the prior calendar year 2017

1. Date filed: February 27, 2018
2. Name of company(s) covered by this certification: Rock County Broadband Alliance, LLC
3. Form 499 Filer ID: 831775
4. Name of signatory: Shirley Flanagan
5. Title of signatory: Customer Service Manager
6. Certification:

I, Shirley Flanagan, 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 Commission's CPNI rules. See 47 C.F.R. § 64.2001 *et seq.*

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 Commission's rules.

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

The company has not received any customer complaints in the past year 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 truthful and accurate statements to the Commission. The company also acknowledges that false statements and misrepresentations to the Commission are punishable under Title 18 of the U.S. Code and may subject it to enforcement action.

Signed

\_\_\_\_\_

**Attachments:**    Accompanying Statement explaining CPNI procedures  
                         Explanation of actions taken against data brokers (if applicable)  
                         Summary of customer complaints (if applicable)

## **ROCK COUNTY BROADBAND ALLIANCE, LLC**

### **STATEMENT EXPLAINING HOW THE COMPANY'S OPERATING PROCEDURES ENSURE COMPLIANCE WITH THE FCC'S CPNI RULES**

#### **I. Customer Proprietary Network Information ("CPNI")**

CPNI is defined in Section 222(f) of the Communications Act as (A) information that relates to the quantity, technical configuration, type, destination, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and (B) information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier (except that CPNI does not include subscriber list information).

Generally, CPNI includes personal information regarding a consumer's use of his or her telecommunications services. CPNI encompasses information such as: (a) the telephone numbers called by a consumer; (b) the telephone numbers calling a customer; (c) the time, location and duration of a consumer's outbound and inbound phone calls, and (d) the telecommunications and information services purchased by a consumer.

Call detail information (also known as "call records") is a category of CPNI that is particularly sensitive from a privacy standpoint and that is sought by pretexters, hackers and other unauthorized entities for illegitimate purposes. Call detail includes any information that pertains to the transmission of a specific telephone call, including the number called (for outbound calls), the number from which the call was placed (for inbound calls), and the date, time, location and/or duration of the call (for all calls).

#### **II. Use and Disclosure of CPNI Is Restricted**

The Company recognizes that CPNI includes information that is personal and individually identifiable, and that privacy concerns have led Congress and the FCC to impose restrictions upon its use and disclosure, and upon the provision of access to it by individuals or entities inside and outside the Company.

The Company has designated a CPNI Compliance Officer who is responsible for: (1) communicating with the Company's attorneys and/or consultants regarding CPNI responsibilities, requirements and restrictions; (2) supervising the training of Company employees and agents who use or have access to CPNI; (3) supervising the use, disclosure, distribution or access to the Company's CPNI by independent contractors and joint venture partners; (4) maintaining records regarding the use of CPNI in marketing campaigns; and (5) receiving, reviewing and resolving questions or issues regarding use, disclosure, distribution or provision of access to CPNI.

Company employees that may deal with CPNI have been informed that there are substantial federal restrictions upon CPNI use, distribution and access. In order to be authorized to use or access the Company's CPNI, employees must receive training with respect to the requirements of Section 222 of the Communications Act and the FCC's CPNI Rules (Subpart U of Part 64 of the FCC Rules).

### **III. Use of CPNI in Marketing**

The Company may wish to inform customers of new, enhanced or beneficial features or services to customers. Information in the Company database will be used in order to determine which customers may be contacted. Before doing so, the customer must have granted the Company permission to use this information for marketing purposes. This information is legally referred to as Customer Proprietary Network Information or CPNI.

#### **Customer Notification**

Annually, existing customers are notified via a bill insert that they have the right to restrict the Company's use of the customer's CPNI. Within 30 days of the notification the customer must either call toll free 1-888-271-0717 or e-mail [cpni@alliancecom.net](mailto:cpni@alliancecom.net) to inform the Company that they wish to restrict the use of CPNI. If the customer does not contact the Company they will be granting the Company the right to use the information. The approval or denial will not affect any service and will remain valid for two years or until the customer either revokes or limits the approval or denial.

New customers are notified via information in the New Customer Packet that is mailed to every new customer when they begin service with the Company. This insert contains the same information as the bill insert. New customer CPNI may not be used until 60 days after the customer begins service with the Company to ensure ample time to respond if the customer wishes to restrict use.

#### **Marketing with CPNI**

Only under the direction of the Company's Marketing Department may CPNI be used. Before using CPNI, the specific Marketing Plan must be approved by the CPNI Compliance Officer. The CPNI Compliance Officer and the Marketing Department is responsible for maintaining and updating the customer database that has denied CPNI usage. A new customer database will be generated each time CPNI is used to ensure that only most current approved customers are contacted.

Upon completion of each marketing attempt, a sample of the communicated script, flyer, post card or however the sales information was presented to the customer using CPNI will be saved. Each attempt will also be documented. A description of what products or services were presented in the attempt. This record will be saved for no less than a year.

Each year the CPNI Compliance Officer and the Marketing Department will review CPNI procedures and policies. The CPNI Compliance Officer and the Marketing Department will review how CPNI rights are communicated to customers. The CPNI Compliance Officer and the Marketing Department will also review the methods of communicating this information.

Any instance where the Company's CPNI procedures have not worked properly will be reported to the CPNI Compliance Officer immediately.

#### **IV. Protection of CPNI**

Customer identity is authenticated prior to disclosing CPNI based on a customer-initiated telephone contact, online account access or in-store visit.

Call Detail Information may only be released by 1) mailing or emailing the CDR to the address (physical or electronic) of record or 2) confirming the customer's identity in person with a valid, government-issued ID.

The Company may permit its customers to establish online accounts, but must require a password to be furnished by the customer before he or she can access any CPNI in his or her online account.

If the customer is able to provide to the Company during a customer-initiated telephone call, all of the call detail information necessary to address a customer service issue (*i.e.*, the telephone number called, when it was called, and, if applicable, the amount charged for the call) without Company assistance, then the Company may take routine customer service actions related to such information. (However, under this circumstance, the Company may not disclose to the customer any call detail information about the customer account other than the call detail information that the customer provides.)

The Company will provide a customer's phone records or other CPNI to a law enforcement agency in accordance with applicable legal requirements.

The Company retains all customer passwords in secure files that may be accessed only by authorized Company employees who need such information in order to authenticate the identity of customers.

When an existing customer calls the Company to inquire about or order new, additional or modified services (in-bound marketing), the Company may use the customer's CPNI other than call detail CPNI to assist the customer for the duration of the customer's call if the Company provides the customer with the oral notice required by Sections 64.2008(c) and 64.2008(f) of the FCC's Rules and after the Company authenticates the customer.

The Company's employees may use CPNI to initiate, render, bill and collect for telecommunications services. The Company may obtain information from new or existing customers that may constitute CPNI as part of applications or requests for new, additional or modified services, and its employees may use such customer information (without further customer approval) to initiate and provide the services. Likewise, the Company's employees may use customer service and calling records (without customer approval): (a) to bill customers for services rendered to them; (b) to investigate and resolve disputes with customers regarding their bills; and (c) to pursue legal, arbitration, or other processes to collect late or unpaid bills from customers.

Company employees are required to notify the CPNI Compliance Officer of any access or security problems they encounter with respect to files containing CPNI.

The Company will notify customers immediately of certain changes in their accounts that may affect privacy or security matters.

a. The types of changes that require immediate notification include: (a) change or request for change of the customer's password; (b) change or request for change of the customer's address of record; (c) change or request for change of any significant element of the customer's online account; and (d) a change or request for change to the customer's responses with respect to the back-up means of authentication for lost or forgotten passwords.

b. The notice may be provided by a written notice mailed to the customer's address of record (to the customer's prior address of record if the change includes a change in the customer's address of record).

c. The notice must identify only the general type of change and must not reveal the changed information.

The Company must provide an initial notice to law enforcement and a subsequent notice to the customer if a security breach results in the disclosure of the customer's CPNI to a third party without the customer's authorization.

a. As soon as practicable (and in no event more than seven (7) days) after the Company discovers that a person (without authorization or exceeding authorization) has intentionally gained access to, used or disclosed CPNI, the Company must provide notification of such breach to the United States Secret Service and to the Federal Bureau of Investigation.

## **V. Disciplinary Procedures**

The Company has informed its employees that it considers compliance with the Communications Act and FCC Rules regarding the use, disclosure, and access to CPNI to be very important.

Violation by Company employees of such CPNI requirements will lead to disciplinary action (including remedial training, reprimands, unfavorable performance reviews, probation, and termination), depending upon the circumstances of the violation (including the severity of the violation, whether the violation was a first time or repeat violation, whether appropriate guidance was sought or received from the CPNI Compliance Officer, and the extent to which the violation was or was not deliberate or malicious).

**ROCK COUNTY BROADBAND ALLIANCE, LLC**

**STATEMENT OF ACTIONS TAKEN AGAINST DATA BROKERS**

- A. During Calendar Year 2017, the Company has instituted the following proceeding, or filed the following petitions, against data brokers before the Federal Communications Commission:

NONE

- B. During Calendar Year 2017, the Company has instituted the following proceeding, or filed the following petitions, against data brokers before the Minnesota Public Utilities Commission:

NONE

- C. During Calendar Year 2017, the Company has instituted the following proceeding, or filed the following petitions, against data brokers before the following federal or state courts:

NONE

**ROCK COUNTY BROADBAND ALLIANCE, LLC**

**SUMMARY OF CUSTOMER COMPLAINTS  
REGARDING UNAUTHORIZED RELEASE OF CPNI**

- A. During Calendar Year 2017, the Company has received the following number of customer complaints related to unauthorized access to, or disclosure of, CPNI due to improper access by Company employees:

NONE

- B. During Calendar Year 2017, the Company has received the following number of customer complaints related to unauthorized access to, or disclosure of, CPNI due to improper disclosure to individuals not authorized to receive the information:

NONE

- C. During Calendar Year 2017, the Company has received the following number of customer complaints related to unauthorized access to, or disclosure of, CPNI due to improper access to online information by individuals not authorized to view the information:

NONE

- D. During Calendar Year 2017, the Company has become aware of the following processes that pretexters are using to attempt to access its CPNI:

NONE