Annual 47 CFR § 64.2009(e) CPNI Certification Template

EB Docket 06-36

Annual 64.2009(e) CPNI Certification for 2019 covering the prior calendar year 2018

1. Date filed: February 27, 2019

2. Name of company(s) covered by this certification: Bijou Telephone Co-Op Association Inc

3. Form 499 Filer ID: 808874

4. Name of signatory: Brian Creveling

5. Title of signatory: General Manager/EVP

6. Certification:

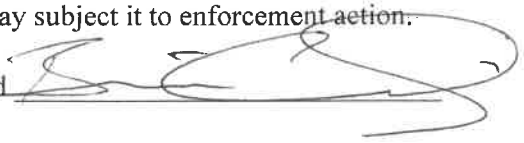
I, Brian Creveling, certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. *See* 47 CFR § 64.2001 *et 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, safeguards, recordkeeping, and supervisory review) set forth in section 64.2001 *et seq.* of the 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 Commission against data brokers) against data brokers in the past year. [NOTE: If you reply in the affirmative, provide an explanation of any actions taken against data brokers.]

The company has not received customer complaints in the past year concerning the unauthorized release of CPNI. [NOTE: If you reply in the affirmative, provide a summary of such complaints. This summary must include the number of complaints, broken down by category or complaint, e.g., instances of improper access by employees, instances of improper disclosure to individuals not authorized to receive the information, or instances of improper access to online information by individuals not authorized to view the information.]

The company represents and warrants that the above certification is consistent with 47 CFR § 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)

ANNUAL 47 C.F.R. SECTION 64.2009 CPNI OPERATING PROCEDURE COMPLIANCE STATEMENT EB DOCKET 06-36

This Operating Procedures Compliance Statement for Bijou Telephone Co-Op Association Inc (the "Company") explains how the Company's procedures ensure that the Company is in compliance with the requirements set forth in Section 64.2009 of the Commission's rules.

Every employee of the Company has a duty to protect the confidentiality of CPNI. A violation of the Company's operating procedures will result in disciplinary action. For a first violation, an employee will be given a warning and the violation will be noted on the employee's record. An employee will be subject to termination of employment for a second violation.

The service categories provided by the Company include local exchange telephone service and DSL access service. It is the Company's policy to NOT use CPNI for any sales or marketing purpose. Specifically, use of CPNI obtained from the Company's provision of one service category to market a second service category to individuals or businesses that are not already customers of that second service category is strictly prohibited.

All Company employees will be trained annually on the Operating Procedures for properly safeguarding all CPNI. The Company holds periodic training sessions to train employees as to when they are and are not authorized to us or disclose CPNI, followed by a supervisory review process regarding compliance with CPNI rules. The Company also sends via company email information to employees relating to CPNI compliance

No Company employee shall disclose CPNI to any Company affiliate or other third party unless such disclosure is required by a lawful subpoena or is used in accordance with Section 64.2009. A Company employee that receives or obtains CPNI for the purpose of providing any telecommunications service shall use the information only for such purpose and shall not use such information for any other purposes.

The Company has developed, through is operating procedures, extensive safeguards that have reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI. Company employees are following procedures designed to authenticate all customers prior to disclosing CPNI based on customer-initiated telephone contact or office visit.

A Company employee shall disclose CPNI only upon an affirmative request by the customer and only after validating that the person requesting the information is the person authorized to discuss CPNI. The validation process must, at a minimum, include asking the person requesting CPNI for a password. If a password cannot be provided by the customer, the Company may disclose call detail information by sending it to the customer's address of record or by calling the customer at the telephone number of record. The customer can also present a valid photo ID in a retail location that matches the customer's account information.

The Company will notify a customer immediately of account activity involving a change to an address of record. Notification may be sent by email, voicemail, text message or US Mail to both the customer's prior and updated address of record.

Notice to customers of their right to restrict use of, disclosure of, and access to their CPNI is provided prior to solicitation for customer approval.

In establishing a password, the Company authenticates the customer without the use of readily available biographical information or account information. The Company has a back- up plan in the event of a lost or forgotten password. However, if a customer cannot provide the correct password or the correct response for the back-up authentication method, the customer must establish a new password.

As required by CPNI rules and as outlined in the Company's operating procedures law enforcement notification procedures are strictly adhered to. Should any breach of CPNI integrity be discovered, the Company will develop and maintain a record as to the date of the breach discovery, who discovered the breach, and the resulting notifications to the United State Secret Service and the Federal Bureau of Investigation no later than 7 days from the date of the discovery of the breach. The records of these discovered breaches will be maintained and held by the Company for no less than 3 years.

Signed _____ Date 2/27/19

Brian Creveling, General Manager/EVP