

**Certification of Customer Proprietary Network Information (CPNI) Filing  
covering calendar year 2018**

**Reference: EB Docket 06-36**

**Date Filed: Feb 15, 2019**

**Company: PBN, LLC**

**Form 499 Filer ID: 830135**

**Name of Signatory: William W B Fogle**

**Title of Signatory: Vice-President**

I, William W.B. Fogle, Vice-President of Pierce Telephone Co., Inc. hereby certify that I am an officer and have personal knowledge the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules.

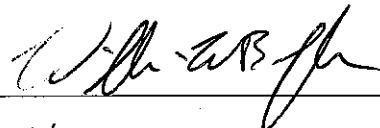
Attached to this certification is an accompanying statement explaining how the company's procedures ensure that the company is in compliance with the requirements, training, safeguards, recordkeeping and review set forth in the rules.

The company has not taken actions 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 that the above certification is truthful and accurate statements.

Signed: \_\_\_\_\_



Printed Name: \_\_\_\_\_

William W B Fogle

Date: \_\_\_\_\_

2/13/19

Attachment: Accompany statement and Operating Procedures

**Customer Proprietary Network Information (CPNI)  
Documentation  
For**

**Pierce Telephone Co., Inc.  
Nebraska Long Distance /dba Pierce Long Distance  
PBN LLC**

**112 S 5<sup>th</sup>, PO Box 113  
Pierce, NE 68767**

- CPNI rules are reviewed on a regular basis with employees that have access to CPNI.
- Employees with access to CPNI have been trained on when they are, and are not, authorized to use CPNI.
- Company does not provide CPNI to third parties.
- Company has a defined disciplinary process in place for violations and for improper use of any customer information, which would include CPNI.
- Currently, our company markets a product or service to its entire customer base or it uses the "total service approach" which allows it to use CPNI to market offerings related to the customer's existing service to which the customer currently subscribes.

If, in the future, the company wants to use CPNI to market outside of the total service approach, a process will be developed for notifying customers of their CPNI rights and for requesting approval to use CPNI. At that time a process will, also, be established for noting customer accounts when notification is given and the approval/denial status on each customer account.

## **OPERATING PROCEDURES FOR COMPLIANCE WITH CPNI RULES**

**Pierce Telephone Co., Inc.**

**Nebraska Long Distance, LLC dba/Pierce Long Distance Company**

**PBN LLC**

The following implemented procedures applies to Pierce Telephone Co., Inc., Nebraska Long Distance LLC dba/Pierce Long Distance Co., and PBN LLC to ensure compliance with Part 64 of Title 47 of the Code of Federal Regulations, Customer Proprietary Network Information (CPNI)

### **Compliance Officer**

The Company has appointed a CPNI Compliance Officer. The Compliance Officer is responsible for ensuring that the Company is in compliance with all of the CPNI rules. The Compliance Officer is also the point of contact for anyone (internally or externally) with questions about CPNI.

### **Employee Training**

The Compliance Officer arranges for the training of employees on an annual basis, and more frequently as needed. Any new employee is trained when hired by the Company. The training includes, but is not limited to, when employees are and are not authorized to use CPNI, and the authentication methods the company is using. The detail of the training can differ based on whether or not the employee has access to CPNI.

After the training, all employees are required to sign a certification that they have received training on the CPNI rules, that they understand the Company's procedures for protecting CPNI and they understand the Company's disciplinary process for improper use of CPNI. Each employee is informed as to where the company's CPNI manual, rules, and information regarding which customers have opted-out is located. All customers who have opted-out are also flagged on their account.

Employees are instructed that if they ever have any questions regarding the use of CPNI, if they are aware of CPNI being used improperly by anyone or if they encounter someone other than the authorized person on a customer's account trying to access CPNI that they should contact the Compliance Officer immediately. The Compliance Officer will then determine what action needs to be taken.

### **Disciplinary Process**

The Company has established a specific disciplinary process for improper use of CPNI. An employee who violates and improperly uses any CPNI information will correct the problem with the customer personally. As stated in the employee handbook, disciplinary action is based on the type and severity of the violation and could include any or a combination of the following: retraining the employee on CPNI rules, notation in the employee's personnel file, verbal warning, formal written reprimand, suspension with or without pay or termination of employment.

The disciplinary process is reviewed with all employees and they must sign a certification on an annual basis that they understand the consequences.

A copy of the Company's disciplinary process is in each employee handbook and in the CPNI manual.

### Customer Notification and Request for Approval to Use CPNI

The company has provided notification to its customers of their CPNI rights and has asked for the customer's approval to use CPNI via the opt-out method. A copy of the notification is also attached to the application provided to all new customers that sign up for service. The Company sends an annual notice to all customers and retains the CPNI notifications on file.

Those customers who choose to opt-out have their account records flagged with an opt-out status that is displayed as soon as the customer's account is accessed so that employees can readily identify customers that have restricted the use of the CPNI.

For the customers that have opted-out and said the Company cannot use their CPNI, that decision will remain valid until the customer changes it. The Company retains those opt-out records on file until revoked. The company sends the opt-out notice annually to those customers that have not previously opted out.

The company does not share CPNI with any joint venture partner, independent contractor or any third party. The company will provide written notice within 5 business days to the FCC of any instance where the opt-out mechanisms do not work properly.

A copy of all notifications are kept with the CPNI official files.

### Marketing Campaigns

The Company has established a supervisory review process for any outbound marketing that it does. If the Compliance Officer must review the campaign and all materials to ensure that it is in compliance with the CPNI rules.

Even though the Company does not use CPNI for marketing campaigns, the company has a process for maintaining a record of any marketing campaign which uses customers CPNI. The record will include a description of the campaign, the specific CPNI that was used in the campaign, and what products and services were offered as part of the campaign.

Customers will still receive monthly bill messages, inserts, newsletters, and other publications that are sent to all customers.

### Authentication

The Company does not disclose any CPNI until the customer has been appropriately authenticated as follows:

**In-office visit** - the customer must provide a valid photo ID matching the customer's account information

**Customer-initiated call** - the customer must provide his/her pre-established password and must be listed as a contact on the account.

If the customer wants to discuss call detail information which requires a password, the following guidelines are followed:

If the customer can provide all of the call detail information (telephone number called, date of call, place called and the amount of the call) necessary to address the customer's issue, the company will continue with its customer care procedures.

If the customer cannot provide all of the call detail information to address the customer's issue, the company will: (1) call the customer back at the telephone number of record, (2) send the information to the address of record, or (3) ask the customer to come into the office and provide a valid photo ID.

### Notification of Account Changes

The Company promptly notifies customers whenever a change is made to any of the following:

- Password
- Address of record

The notification to the customer will be made either by a company-originated call or voicemail message to the telephone number of record.

The company has a process for tracking when a notification is required by reviewing the individual service orders prior to updating the account. A automated process generates the required notifications to be mailed.

### Notification of Breaches

Employees will immediately notify the Compliance Officer of any indication of a breach. If it is determined that a breach has occurred, the Compliance Officer will do the following:

Notify the United States Secret Service (USSS) and the Federal Bureau of Investigation (FBI) as soon as practicable, but in no event later than 7 business days after determination of the breach. The notification will be via the FCC link at <http://www.fcc.gov/eb/cpni>.

Notify customers only after 7 full business days have passed since notification to the USSS and the FBI, unless the USSS or FBI has requested an extension.

If there is an urgent need to notify affected customers or the public sooner to avoid immediate and irreparable harm, it will be done only after consultation with the relevant investigating agency.

Maintain a record of the breach, the notifications made to the USSS and FBI, and the notifications made to customers. The record should include dates of discovery and notification, a detailed description of the CPNI that was the subject of the breach, and the circumstances of the breach.

Include a summary of the breach in the annual compliance certificate filed with the FCC.

### Annual Certification

The Compliance Officer will file a Compliance Certification with the FCC by March 1 of each year for data pertaining to the previous calendar year.

### Record Retention

The Company retains all information regarding CPNI in a CPNI file in the Compliance Officer's office. Following is the minimum retention period we have established for specific items:

- CPNI notification-two years
- Records of Opt-out - until revoked
- Marketing Campaigns - one year
- Breaches - two years
- Annual certification - seven years
- Employee Training Certification - two years
- All other information - two years

### Miscellaneous

The Company's CPNI policies include reasonable measures to discover and protect against activity that is indicative of pretexting, as well as any other unauthorized attempts to access CPNI. Employees are instructed to notify the CPNI Compliance Officer immediately of any suspicious activity who will then determine what action needs to be taken.