

Nebraska Central Telephone Company

22 LaBarre St PO Box 700 Gibbon, NE 68840-0700

Phone: (308) 468-6341 Fax: (308) 468-9929 www.nctc.net

February 22, 2018

Marlene H. Dortch, Secretary  
Office of the Secretary  
Federal Communications Commission  
445 12<sup>th</sup> Street, SW  
Washington, D.C. 20554

RE: EB Docket No. 06-36  
Annual CPNI Certification

Dear Ms. Dortch:

Attached is the annual CPNI certification filing covering the year of 2017, pursuant to 47 C.F.R § 64.2009(e), for Nebraska Central Telephone Co 802560.

Sincerely,

A handwritten signature in black ink that reads "Andrew D Jader". The signature is written in a cursive, flowing style.

Andrew D Jader  
Vice President of Administration

Attachment

# **Annual 47 C.F.R. § 64.2009(e) CPNI Certification Template**

## **EB Docket 06-36**

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

1. Date filed: February 22, 2018
2. Name of company(s) covered by this certification: The Nebraska Central Telephone Company. dba Nebraska Central Telephone Co.
3. Form 499 Filer ID: 802560
4. Name of signatory: Andrew D. Jader
5. Title of signatory: Vice President - Administration
6. Certification:

I, Andrew D. Jader 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.*

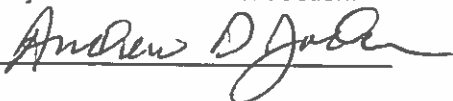
Attached to this certification is an accompanying statement explaining how the company's procedures ensure that the company is in compliance with the requirements (including those mandating the adoption of CPNI procedures, training, safeguards, recordkeeping, and supervisory review) set forth in section 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.

The company has not received 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

## OPERATING PROCEDURES FOR COMPLIANCE WITH CPNI RULES

The Nebraska Central Telephone Company (the "Company") has implemented the following procedures to ensure that it is compliant with Part 64 of Title 47 of the Code of Federal Regulations, Subpart U – Customer Proprietary Network Information (CPNI), § 64.2001 through § 64.2011.

### Compliance Officer

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

### Personnel Training

The Compliance Officer arranges for the training of all personnel within the Company on an annual basis or more frequently if needed. All new personnel are trained and given a Company Consumer Protection Policy Manual, which includes the Company's CPNI policy, when hired by the Company. The training includes, but is not limited to, when personnel are and are not authorized to use CPNI, and the authentication methods the Company uses. The detail of the training can differ based on whether or not the personnel have access to CPNI.

After the training, all personnel are required to sign a certification that they have received a manual and have been trained 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.

Personnel are instructed that if they ever have any questions regarding the use of CPNI, or if they are aware of CPNI being used improperly by anyone, they should contact the Compliance Officer immediately.

### Disciplinary Process

The Company has established a specific disciplinary process for improper use of CPNI. The disciplinary action is based on the type and severity of the violation and could include any or a combination of the following: retraining the person on CPNI rules, notation in the person's personnel file, formal written reprimand, suspension or termination.

The disciplinary process is reviewed with all personnel and is outlined in the Company's Consumer Protection Policy, which all personnel are given.

### 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 their customer's approval to use their CPNI via the opt-out method. The Company sends the opt-out notice every two years to those customers that have not previously opted out. The most recent customer notices regarding CPNI were mailed to customers during January 2016. A copy of the notification is also provided to all new customers. A copy of the most recent notification is kept with the files that are maintained by the Compliance Officer.

The status of a customer's CPNI approval is prominently displayed as soon as the customer's account is accessed so that personnel can readily identify customers that have restricted the use of their 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 will provide written notice, in the form of a letter, within five business days to the FCC of any instance where the opt-out mechanisms do not work properly, to such a degree that consumers' inability to opt-out is more than an anomaly. The Company will submit a notice even if other opt-out methods are offered. The notice will include the company name, a description of the opt-out mechanism(s) used, the problem(s) experienced, the remedy proposed and date implemented, whether the relevant state commission(s) has been notified and whether it has taken any action, a copy of the notice provided to the customers, and contact information.

### Marketing Campaigns

The Company does not disclose or allow access by third parties to CPNI. Sales personnel must obtain supervisory approval of any proposed outbound marketing request for customer approval. The CPNI Compliance Officer reviews all proposed outgoing campaigns and materials to ensure that they are compliance with the CPNI rules.

Company marketing campaigns and a record of their compliance are recorded and maintained for a period of two years. The record includes a description of each campaign, if CPNI was used and, if so, the specific CPNI that was used and what products and services were offered as part of the campaign.

### 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 and be listed as a contact on the account.

**Customer-initiated call** - the caller must be listed as a contact on the account and be able to provide the answer to the pre-established question of what the last four digits of their Social Security or Federal ID Number is. The account contact information is located on the CPNI Questions Screen accessed on a customer's account.

If the customer wants to discuss call detail information the following guidelines are followed:

- If the customer can provide all of the call detail information (telephone number called, when it was called, and the amount of the call) necessary to address the customer's issue, the personnel will continue with routine customer care procedures.
- If the customer cannot provide all of the call detail information to address the customer's issue, the personnel 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.

**Online access** – A password is set up at the time service is established for new customers and after proper authentication for existing customers. The customer is authenticated without the use of biographical or account information by having the customer come into the business office with a valid photo ID, calling the customer at the telephone number of record or by sending a randomly-generated PIN # to the customer's address of record. The customer is then only allowed online access through the use of a password that is not based on readily available biographical or account information.

For instances of lost or forgotten passwords, a backup authentication method is available and can be generated by the customer after the customer accesses their online account for the first time. The backup authentication method is a non-biographical non-account based question that is selected by the customer from a pre-established list. In the event that an online account has five consecutive unsuccessful log-in attempts, the account will be blocked until the customer is again authenticated without using biographical or account information.

### Notification of Account Changes

The Company's computer system is programmed to automatically generate and print a notice anytime one of the following changes has been made to an account:

- Service or billing name
- Contact name (and/or) ID #
- Address of record

The notice advises that a change has occurred to an account but does not advise the changed information. The notice is mailed out to the postal address of record the same day that the change occurs. A record of that notice is automatically generated into an e-mail which is sent to the CPNI Compliance Officer for review and tracking purposes.

The Company computer system is programmed to send out an electronic notice to the e-mail address of record any time an online account is added, changed or has had anything downloaded. The notice advises that a change has occurred without advising what the changed information is. An electronic record of that notice is generated into an activity log which can be accessed through the company's computer system for reviewing and tracking purposes.

### Notification of Breaches

Personnel will immediately notify the Compliance Officer and fill out a statement of breach if there is any indication that a breach may have occurred. 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

A company 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 filed in the possession of the Compliance Officer. Following is the minimum retention period the Company has established for specific items:

- CPNI notification and records of approval two years
- Marketing campaigns – two years
- Breaches – two years
- Annual certification – five years
- Employee training certification – one year beyond completion of employment
- All other information – two years