

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 28, 2019
2. Name of company covered by this certification: Northwestern Indiana Telephone Company, Inc
3. Form 499 Filer ID: 803475
4. Name of signatory: Thomas C Long
5. Title of signatory: President/COO
6. Certification:

I, Thomas C Long, 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.

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 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  [Signature of an officer, as agent of the carrier]

Attachments: Accompanying Statement explaining CPNI procedures

Attachment Accompanying Statement of Company Procedures

Per the FCC CPNI rules [47 CFR §64.2009(e)] and as referenced in the attached signed certification, (Insert Company Name), herein referenced as the Company hereby certifies that the Company [and its affiliates] is in compliance with the FCC CPNI rules and has outlined some of the important operating procedures below in order to ensure the Company's compliance in the protection of CPNI:

1. CPNI manual has been updated in order to account for all FCC CPNI rules, including the recent revisions, and has been adopted by our Company's board
2. CPNI Compliance officer has been designated to oversee all CPNI duties, training, and activity
 - o Established an outbound marketing supervisory review process for the use of CPNI
 - o Records are maintained for any marketing campaigns that utilize customers' CPNI for a minimum of one year
3. Employees have been trained on when they are, and are not, authorized to use or disclose CPNI
 - o Disciplinary process has been defined and is in place for violations and/or breaches of CPNI
4. Carrier authentication requirements have been met
 - o All customer during a customer-initiated telephone call are authenticated as being an authorized account contact before discussing CPNI (non-call detail or call detail) without utilizing readily available biographical or account information as defined by the FCC
 - o Call detail is only released to customers during customer-initiated telephone contact if a password is provided. If the requesting customer does not provide a password, only the following FCC approved methods are permitted for the release of the requested call detail:
 - Sending the requested detail to the address of record (only a physical or email address associated with that particular account that has been in our company files for at least 30 days)
 - Calling the customer back at the telephone of record (only disclosing if the customer was authenticated as being an authorized account contact)
 - Having customer come in to Company's office and provide a valid government issued photo ID
5. Notice to customer of account change as customers are notified immediately when a customer creates or changes one of the following:
 - o password
 - o customer response to a back-up means of authentication for lost or forgotten passwords
 - o online account
 - o address of record
6. Notice of unauthorized disclosure of CPNI, a notification process is in place in order to notify both law enforcement and customer(s) in the event of a CPNI breach within the timeline specified by the FCC
7. CPNI is strictly not used in Marketing campaigns
 - o Billing system has the ability to display customer's opting status.
 - o Compliance officer approves marketing campaigns to assure CPNI is not being used.
 - o Marketing retains records of all campaigns.
8. Additional protection measures are taken above and beyond the current FCC CPNI rules
 - o Company takes reasonable measures to discover and protect against activity that is indicative of pretexting
 - o Company maintains security of all CPNI, including but not limited to:
 - Documents containing CPNI are shredded
 - Computer terminals are locked when employee is not at the station