

Annual 47 CFR § 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: 3/1/2018
2. Name of company(s) covered by this certification: Wikstrom Telephone Company Inc.
3. Form 499 Filer ID: 801048
4. Name of signatory: Leslie B. Wikstrom
5. Title of signatory: Vice President
6. Certification:

I, Leslie B Wikstrom, 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  [Signature of an officer, as agent of the carrier]

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

STATEMENT OF COMPLIANCE

The operating procedures of Wikstrom Telephone Co. Inc. ensure compliance with the FCC's CPNI Rules. Such procedures are as follows:

Use of CPNI in Marketing

Our company does not use CPNI in any of its marketing efforts, and does not permit the use of, or access to, customer CPNI by our affiliates or any third parties. We use, disclose or permit access to CPNI only for the purposes permitted under 47 U.S.C. Sections 222(c)(1) and (d).

CPNI Safeguards

Our company has designated a compliance officer to maintain and secure the company's CPNI records and to supervise training of all company employees.

Our company trains its personnel as to when they are, and are not, authorized to use or disclose CPNI, and we have an express disciplinary process in place if the rules are violated.

Our company authenticates the identity of a customer prior to disclosing CPNI based on a customer-initiated telephone contact or in-store visit.

Our company discloses call detail information (CDI) in a customer-initiated call only: after the customer provides a pre-established password; or, at the customer's request, by sending the CDI to the customer's address of record; or by calling back the customer at his or her telephone number of record; or by asking the customer questions about their account only they and Wikstrom Telephone Co. should know and that most other people would not know.

Our company discloses CPNI to a customer in person at our retail location only when the customer presents a valid photo ID and the ID matches the name on the account.

Our company establishes passwords with customers in order to authenticate customers. Neither passwords nor the backup method for authentication rely on customers' readily available biographical information.

Our company does not have online accounts at this time. However, we do have procedures in place to protect CPNI if we should ever decide to offer online account information. These procedures include establishing password protection for customers' online accounts.

CPNI Recordkeeping and Reporting

Our company is prepared to notify the U.S. Secret Service and FBI within seven business days after the occurrence of an intentional, unauthorized (or exceeding authorization), access to, use of, or disclosure of CPNI. We may also notify the customer of such breach, after consulting with the investigatory agency(ies), if we believe there is an extraordinarily urgent need to notify a customer (or class of customers) in order to avoid immediate or irreparable harm. We will notify the customer of the breach after 7 business days following notification to the FBI and Secret Service, if such agencies have not requested that we postpone disclosure to the customer.

Our company will maintain records of any discovered breaches, notices to the Secret Service and FBI, and their responses, for at least two years.