

Annual 47 C.F.R. § 64.2009(e) CPNI Certification
EB Docket 06-36

Annual EB Docket No. 06-36, Certification for 2018 covering the prior Calendar Year 2017

Date: February 8, 2018

This letter serves as the below-named Company's "Certification of CPNI Filing for Calendar Year 2017", as ordered in EB Docket No. 06-36.

Company Name: City of Windom

Address: 444 9th Street, PO Box 38, Windom, MN 56101

Form 499 Filer ID: 825807

Name and Title of Signatory: Steve Nasby City Administrator

Certification:

I, Steve Nasby certify that I am an officer of the Company named above, and that, based on my personal knowledge and acting as an agent for the Company, the Company has established operating procedures that are adequate to ensure compliance with the Commission's Customer Proprietary Network Information ("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, recordkeeping, and supervisory review) set for in section 64.2001 *et seq.* of the Commission's rules.

The Company has not taken any action (proceedings instituted or petitions filed by the Company at state commissions, the court system, or the FCC) against data brokers in the past year.

The Company has not received any customer complaints in the past year concerning 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.



Company Officer

Dated: 8 Feb 2018

Attachment - Statement of Compliance

STATEMENT OF COMPLIANCE

The operating procedures of the City of Windom 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 will use, disclose or permit access to CPNI only for the purposes permitted under 47 U.S.C. Sections 222 (c) (1) and (d).

Our company has a supervisory review process regarding our compliance with the FCC's CPNI rules for any outbound marketing efforts. We require sales personnel to obtain supervisory approval of any proposed outbound marketing request for customer approval.

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. Employees attended a CPNI training titled "FCC Latest Customer Propriety Network Information Requirements".

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.

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

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

Our company will only disclose call detail information (CDI) in a customer-initiated call: 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 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 notifies a customer immediately of changes in: a customer's password, a customer's response to back-up means of authentication or address of record.

CPNI Recordkeeping and Reporting

Our company is prepared to provide the FCC with written notice, within five business days of any instance where the "opt out" mechanisms do not work properly.

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.