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: February 27, 2018

2. Name of company(s) covered by this certification: All West Utah

3. Form 499 Filer ID: 809006

4. Name of signatory: Bridget Watkins

5. Title of signatory: Vice President Marketing and Sales

6. Certification:

I, Bridget Watkins, 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 Bridget Watkins [*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 EXPLAINING HOW THE COMPANY'S OPERATING PROCEDURES ENSURE COMPLIANCE WITH THE FCC'S CPNI RULES

All West Utah (the "Company") does not use, disclose, or permit access to Customer Proprietary Network Information ("CPNI") except as permitted or required by law pursuant to 47 USC §222, and the CPNI Rules, 47 CFR §64.2001-2011. The Company's operating procedures, as summarized below, ensure the Company is in compliance with the CPNI Rules in the protection of CPNI:

The Company recognizes that CPNI includes information that is personal and individually identifiable, and that use, disclosure of, and access to CPNI is restricted by the FCC laws and rules. As a result, the Company has adopted a CPNI Manual that has been reviewed to ensure compliance with the FCC CPNI Rules, and has designated a CPNI compliance officer to oversee all CPNI duties, training, and activity.

The Company may use, disclose, or permit access to CPNI for the purposes of providing or marketing service offerings among the categories of service to which a customer already subscribes from the Company without customer approval.

To the extent the Company provides different categories of service and a customer subscribes to more than one category of service offered by the Company, the Company may share CPNI among the Company's affiliated entities that provide a service offering to the customer. However, when the Company provides different category of services and the customer does not subscribe to more than one offering, the Company will not share CPNI unless the Company has customer approval to do so.

The Company does not use, disclose, or permit access to CPNI to market to a customer any service offerings that are within a category of service to which the customer does not already subscribe from the Company unless the Company has customer approval to do so.

The Company obtains customer approval through written, oral, or electronic methods. It is the Company's policy that it may, subject to opt-out approval or opt-in approval, use CPNI for the purpose of marketing communications-related services to that customer, to the Company's agents and/or its affiliates that provide communications related services. Prior to any solicitation for customer approval of the use or disclosure of CPNI, the Company provides notification to the customer explaining the customer's right to restrict use of, disclosure of, and access to that customer's CPNI. The Company notice complies with all the requirements of 47 CFR 64.2008.

The Company has implemented all of the safeguards required for use of CPNI as set forth in 47 CFR 64.2009, including:

- Implementing a system by which the status of a customer's CPNI approval can be clearly established prior to the use of CPNI. Specifically, the billing/service record system displays "opt-in" or "opt-out" status on the initial screen or pop-up screen.
- Maintaining a training program to ensure that all employees understand their obligations to protect CPNI and the Company's obligation to comply with the CPNI laws and rules. Employees are trained as to when they are and are not authorized to use CPNI. Specifically, employees are trained upon hiring, and annually thereafter.
- Having an established disciplinary process for employee violations or breaches of CPNI policies.
- Maintaining records for at least one year of the Company's and its affiliates' sales and marketing campaigns that use Customer CPNI.

- Establishing a supervisory review process to ensure compliance with outbound marketing situations, including maintaining required records for one year, and requiring supervisory approval of any outbound marketing request for customer approval.
- Annual certification by officer as to Company's compliance with applicable laws and FCC rules.
- Providing written notice as required by federal law and FCC rules in the event the opt-out mechanism do not work properly, to such a degree that a customer's inability to opt-out is more than an anomaly.

It is the Company's policy to take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI. As a result, the Company has implemented the safeguards required for Disclosure of CPNI as set forth in 47 CFR 64.2010, including:

- Requiring all customers to be authenticated prior to disclosing CPNI based on customer-initiated phone calls, online account access, or in-store visit.
- Requiring a password for customer- initiated calls for account information, call detail, and online access. If the customer does not provide the password, the Company will only disclose call detail information by sending it to the customer's address of record, or the customer may be called back at the number of record. If the customer is able to provide call detail information without the Company's assistance, the Company may discuss the call detail information provided by the customer.
- Requiring the customer be authenticated without the use of readily available biographical information or account information, prior to allowing the customer online access to CPNI.
- Requiring a valid photo ID matching the customer's account information prior to disclosing CPNI to a customer at an in-store location.
- Establishing a customer password without the use of readily available biographical information or account information. The Company may create a back-up customer authentication method in the event of a lost password, but such back-up customer authentication method may not prompt a customer for readily available biographical information or account information.
- Notifying customer of account changes whenever a password, customer response to back-up authentication question, online account, or address of record is changed or created or if the account is accessed using a back-up means of authentication.

Finally, in the unlikely event of a breach of its customers CPNI, it is the Company's policy to notify law enforcement and its customers of such breach in compliance with the time frames and the requirements of 47 CFR 64.2011. The Company has implemented a notification process in compliance with federal law and FCC rules.