

ANNUAL 47 C.F.R § 64.2009(e) CPNI CERTIFICATION

EB Docket No. 06-36

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

Date filed: February 20, 2018

Companies covered by this certification:

Waitsfield – Fayston Telephone Co., Inc, d/b/a Waitsfield and Champlain Valley Telecom
Green Mountain Long Distance Service, Inc.

Form 499 Filer ID: 803463/ 817194

Name of signatory: Roger Nishi

Title of signatory: Vice President-Industry Relations

I, Roger Nishi, certify that I am a corporate officer of the companies named above. Acting as an agent of the companies, that I have personal knowledge that the companies have 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 a statement explaining how the companies' procedures ensure that the companies are in compliance with the requirements set forth in section 64.2001 *et seq.* of the Commission's rules.

The companies have not taken any actions (proceedings instituted or petitions filed by a company at either state commissions, the court system or at the Commission) against data brokers in the past year.

The companies have not received any customer complaints in the past year concerning the unauthorized release of CPNI.

The companies represent and warrant that the above certification is consistent with 47 C.F.R. § 1.17, which requires truthful and accurate statements to the Commission. The companies also acknowledge that false statements and misrepresentation to the Commission are punishable under Title 18 of the U.S. Code and may subject it to enforcement action.

Signed 
Roger Nishi, Vice President-Industry Relations

STATEMENT OF FCC CPNI RULE COMPLIANCE

This statement serves to explain how Waitsfield – Fayston Telephone Co., Inc, d/b/a Waitsfield and Champlain Valley Telecom and Green Mountain Long Distance Service, Inc., (the “Companies”) are complying with Federal Communications Commission (“FCC”) rules related to the privacy of customer information. The type of information for which customer privacy is protected by the FCC’s rules is called “customer proprietary network information” (“CPNI”). The FCC’s rules restricting telecommunications company use of CPNI are contained at Part 64, Subpart U of the FCC’s rules (47 C.F.R. § 64.2000-2011).

1. Duty to Protect CPNI

We recognize our duty to protect customer CPNI. We may not disclose CPNI to unauthorized persons, nor may we use CPNI in certain ways without consent from our customers. Before we can provide customers with their own CPNI, we must authenticate the customer.

We recognize that there are a few cases in which we can disclose CPNI without first obtaining customer approval:

- i. Administrative use: We may use CPNI to initiate, render, bill and collect for communications services.
- ii. Protection of carrier and third parties: We may use CPNI to protect the interests of our Companies, such as to prevent fraud or illegal use of our systems and network. Employees are notified of the steps to take, if any, in these sorts of situations.
- iii. As required by law: We may disclose CPNI if we are required to by law, such as through legal process (subpoenas) or in response to requests by law enforcement. Employees are notified of any steps they must take in these situations.

2. Our Use of CPNI in Marketing

The Companies do not use CPNI for marketing purposes except in the following circumstances:

- i. to market services to our existing customers within the categories of service to which the customer already subscribes;
- ii. to market “adjunct-to-basic” services; and
- iii. to provide CPE and call answering, voice mail or messaging, voice storage and retrieval services, fax store and forward, and protocol conversion.

For marketing purposes for which use of CPNI would otherwise require permission from the Customers, the Companies use only Customer billing name and address and/or telephone number without any segregation or refinement based on CPNI. On inbound and administrative calls, however, the Companies may utilize CPNI in its sales and marketing efforts by first requesting permission to do so pursuant to §64.2008(f). In those cases, the

Companies recognizes that permission to use CPNI ends when the call terminates and the Customer is fully informed that he may refuse the permission.

We regularly review our marketing practices to determine when, how and if CPNI is used within the Companies to insure that we remain in compliance with the FCC's CPNI regulations and with our policy as described here in. In the unlikely event that Companies decide to modify its policies for use of CPNI, it will insure that its new policy fully complies with FCC CPNI rules including, but not limited to, tracking and Customer notice provisions contained in §64.2008-2009.

3. Authentication Prior to Disclosure of CPNI

We understand that we are required to determine that any request for CPNI will not be released without authenticating the authority of the requestor to receive such information.

We understand that when a customer calls, we may not release CPNI until we have authenticated the release of the information to the requestor in one of the following ways:

- i. By calling the customer back at the telephone number associated with the communications service;
- ii. By mailing the information to the address of record;
- iii. By releasing it in person following authentication via a valid government-issued photo identification at our office;
- iv. For those customers who have chosen to do so, over the phone following the disclosure of a password.

4. Employee Issues

All of our employees were trained regarding the Companies' CPNI policies prior to the effective date of the most recent CPNI regulations, December 8, 2007. To maintain compliance with FCC rules after December 8, 2007, the Companies developed a manual and identified a compliance officer to address any CPNI-related issues that may arise. The Companies have established procedures and trained employees having access to, or occasion to use customer data, to identify what customer information is CPNI consistent with the definition of CPNI under the FCC's revised CPNI rules.

The Companies have implemented a training procedure for all new hires and contractors regarding the Companies' practices regarding CPNI.

In addition, the Companies have in place an express disciplinary process to address any unauthorized use of CPNI where the circumstances indicate authorization is required under the FCC's CPNI rules.

5. Notifications to Customers

We notify customers when changes have been made to passwords, customer responses to back-up means of authentication (if implemented), addresses of record and authorized users by mailing a notification to the account address of record. The notice does not contain information regarding the changes.

6. Record-Keeping

We maintain the following records in our files for at least two years:

- i. Records relating to the annual mailing of the customer CPNI privacy policy;
- ii. Employee disciplinary records, if applicable; and
- iii. If applicable: 1) records of discovered CPNI breaches 2) notifications to law enforcement regarding breaches, and 3) any responses from law enforcement regarding those breaches.

7. Unauthorized Disclosure of CPNI

We understand that we must report CPNI breaches to law enforcement no later than seven (7) business days after determining the breach has occurred, by sending electronic notification through the link at <http://www.fcc.gov/eb/CPNI/> to the central reporting facility, which will then notify the United States Secret Service (USSS) and the Federal Bureau of Investigation (FBI).

We understand that we may not notify customers or the public of the breach earlier than seven (7) days after we have notified law enforcement through the central reporting facility. If we wish to notify customers or the public immediately, where we feel that there is “an extraordinarily urgent need to notify” to avoid “immediate and irreparable harm,” we inform law enforcement of our desire to notify and comply with law enforcement’s directions.

During the course of the year, we compile information regarding pretexter attempts to gain improper access to CPNI, including any breaches or attempted breaches. We include this information in our annual CPNI compliance certification filed with the FCC.