



1417 Kreskv Ave Ste 1 | Centralia, WA 98531 | www.rainierconnect.com

February 28, 2011

BY ELECTRONIC FILING

Marlene H. Dortch
Office of the Secretary
Federal Communications Commission
445 12th Street, SW Suite TW-A325
Washington DC 20554

RE: EB Docket No. 06-36
REVISED Annual CPNI Certification
Filed in the year 2011 covering the prior calendar year 2010
Mashell Telecom, Inc. d/b/a Rainier Connect
FCC Form 499 Filer ID: 803703

To Whom It May Concern:

Attached is Mashell Telecom, Inc. d/b/a Rainier Connect's Revised CPNI Certification for the year 2011 covering the prior year 2010. The purpose of this filing is to supplement and replace our original filing of this Docket which was filed on January 24, 2011 and posted January 25, 2011. The changes to this revised filing consist of the addition of more detailed information regarding the Company's CPNI compliance policies and procedures.

This revised certification will be filed electronically in the ECFS system.

Please contact me if you have any questions or concerns regarding this filing.

Sincerely,

A handwritten signature in black ink that reads "Mark Carrier".

Mark Carrier
Regulatory & Compliance Manager
Mashell Telecom, Inc. d/b/a Rainier Connect
PO Box 683
Centralia, WA 98531
360-623-4555 - Direct
360-388-6392 - Cell
360-623-1115 - Fax
mark.carrier@rainierconnect.net

cc: Best Copy and Printing, Inc. *via email to* fcc@bcpiweb.com

Annual 47 C.F.R. § 64.2009(e) CPNI Certification

EB Docket 06-36

Annual 64.2009(e) CPNI Certification for 2011 covering the prior calendar year 2010

1. Date filed: 1/24/11, (Revised Filing 2/28/11)
2. Name of company covered by this certification: Mashell Telecom, Inc. d/b/a Rainier Connect
3. Form 499 Filer ID: 803703
4. Name of signatory: Brian Haynes
5. Title of signatory: President / CEO
6. Certification:

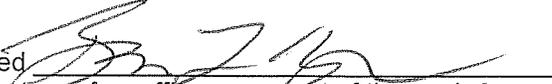
I, Brian Haynes, certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. See 47 C.F.R. § 64.2001 *et seq.*

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 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 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.

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

Attachments:

1. Accompanying Statement explaining CPNI procedures
2. Explanation of actions taken against data brokers (if applicable) (N/A)
3. Summary of customer complaints (if applicable) (N/A)

**STATEMENT OF COMPLIANCE WITH PROTECTION OF
CUSTOMER PROPRIETARY NETWORK INFORMATION RULES
(REVISED)**

Mark Carrier signs this Certificate of Compliance in accordance with Section 222 of the Telecommunications Act of 1996, as amended, 47 USC 222, and the FCC's Code of Federal Regulations (CFR) Title 47 §64.2009, on behalf of **Mashell Telecom, Inc. d/b/a Rainier Connect**. This Certificate of Compliance addresses the requirement of FCC's (CFR) Title 47 §64.2009 that the Company provide both a Certificate of Compliance and a statement accompanying the certificate to explain how its operating procedures ensure compliance with FCC's (CFR) Title 47 §64.2001-2011.

On behalf of the Company, I certify as follows:

1. I am the **Regulatory & Compliance Manager** of the Company.

My business address is:

**1417 Kresky Ave. #1, PO Box 683.
Centralia, WA 98531**

2. I have personal knowledge of the facts stated in this Statement of Compliance. I am responsible for overseeing compliance with the Federal Communications Commission's (FCC) rules relating to customer proprietary network information (CPNI).

3. It is the policy of the Company to comply with the letter and spirit of all laws of the United States, including those pertaining to CPNI contained in Section 222 of the Telecommunications Act of 1996, as amended, 47 USC 222, and the FCC's Code of Federal Regulations (CFR) Title 47 §64.2001-2011 as outlined in the *CPNI Order* and subsequent proceedings. The company follows industry-standard policies and practices to prevent unauthorized access to CPNI by anyone other than the subscriber or the Company.

Some but by no means all of these procedures are provided below in this statement. ***More detailed procedures are listed in the Company's CPNI Compliance Manual and Operating Procedures, which is provided to all employees and on which they receive training.*** Employees are responsible for reading and reviewing the CPNI Manual and to seek clarification from their Manager or the Company's CPNI Compliance Officer regarding any CPNI-related question. The Company does not and has not in the past provided access to CPNI to contractors and third-party vendors, other than for uses authorized by Section 222 of the Communications Act of 1934, as amended, such as assistance with the preparation of the Company's monthly bills to its Customers.

Definition of CPNI

Information obtained by the Company about the Customer and the customer's telecommunications services, (including Interconnected VoIP service), in the course of providing those services. CPNI includes the quantity, technical configuration, type, destination and amount of use of those services.

CPNI Training and Disciplinary Policy

1. The Company provides ongoing training to its personnel regarding when they are authorized to use CPNI, as well as when they are not authorized to use CPNI. However, Company personnel make no decisions regarding CPNI without first consulting with **myself, Customer Service Managers, Kelly Wienholz or Amanda Singleton or Marketing & Commercial Sales Manager, Debbie Reding.** Also included is training regarding the

CERTIFICATE OF COMPLIANCE WITH PROTECTION OF CUSTOMER PROPRIETARY NETWORK INFORMATION RULES (Cont.)

Company's Customer Authentication procedures as well as General CPNI rules and regulations and the Company's own CPNI compliance procedures. The Company has an express disciplinary process in place for personnel who make unauthorized use of CPNI, up to and including termination of employment, if appropriate.

Customer Authentication Procedures

1. Prior to providing any CPNI, including Call Detail Records (CDR) and non-call detail information, all Customers must be properly authenticated prior to disclosing CPNI during Customer initiated phone contact, online account access or an in-store visit.
2. To receive CPNI, including CDR, Customers must use a pre-established password or be able to address the specific service issue they are inquiring about (such as the phone number called, when it was called and, if applicable, the amount charged for the call). In cases of the latter, Company representatives may only address the issues about which the Customer is able to demonstrate knowledge. The Company has established detailed policies for establishment of Customer passwords, which are outlined in its CPNI Policy Manual.
3. If the Customer is unable to provide a correct password, CPNI may be shared by one of the following procedures.
 - a. Calling the Customer back at the telephone number of record.
 - b. Mailing the information to the postal or email address of record, if the address has not been changed in the past 30 days.
 - c. In person upon presentation of a valid photo ID.

Company Use of CPNI

1. The Company has established a system by which the status of a customer's approval for use of CPNI, as defined in 47 USC 222(h)(1), can be clearly established prior to the use of CPNI. The Company uses the "Opt-out" approval process for purposes of obtaining Customers' permission to use CPNI for marketing services outside the category of service(s) a Customer already subscribes to. Customers' records are clearly flagged when a Customer chooses to "Opt-out". Customers are provided notice annually of their right to Opt-out". The Company relies on the involvement of its high-level management to ensure that no use of CPNI is made until a full review of applicable law has occurred.
2. The Company seldom uses CPNI for marketing purposes, but the Company's policy is to maintain records of its own sales and marketing campaigns that use CPNI. The Company will also maintain records of all instances where CPNI is disclosed or provided to third parties if it ever does so, or where third parties are allowed access to CPNI In full compliance with regulations. These records include a description of each campaign, the specific CPNI that was used in the campaign, and the products and services that were offered as a part of the campaign. The Company maintains these records in its offices for a minimum of one year.
3. The Company's policy is to maintain records of customer approval for use of CPNI, as well as notices required by the FCC's regulations, for a minimum of one year. The Company maintains records of customer approval and disapproval for use of CPNI in a readily available location that is consulted on an as-needed basis.

**CERTIFICATE OF COMPLIANCE WITH PROTECTION OF
CUSTOMER PROPRIETARY NETWORK INFORMATION RULES (Cont.)**

4. The Company's policy is to maintain records of a CPNI breach for a minimum of two years. These records will include a description of the steps the company took to prevent the breach, how the breach occurred, the impact of the breach and proof of notification to law enforcement and the customer, if applicable.

5. The Company has a supervisory review process regarding compliance with the FCC's rules relating to protection of CPNI for outbound marketing situations. The purpose of this supervisory review process is to ensure compliance with all rules prior to using CPNI for a purpose for which customer approval is required. Company personnel, prior to making any use of CPNI, must first consult with Customer Service Managers, Kelly Wienholz or Amanda Singleton, Marketing & Commercial Sales Manager, Debbie Reding or me regarding the lawfulness of using the CPNI in the manner contemplated. In deciding whether the contemplated use of the CPNI is proper, Customer Service Managers, Kelly Wienholz or Amanda Singleton, Marketing & Commercial Sales Manager, Debbie Reding or I consult one or more of the following: the Company's own compliance manual, the applicable FCC regulations, the FCC's Compliance Guide, and, if necessary, legal counsel. The Company's sales personnel must obtain supervisory approval from Customer Service Managers, Kelly Wienholz or Amanda Singleton, Marketing & Commercial Sales Manager, Debbie Reding or me regarding any proposed use of CPNI.

6. Further, Customer Service Managers, Kelly Wienholz or Amanda Singleton, Marketing & Commercial Sales Manager, Debbie Reding or I personally oversee the use of opt-in, opt-out, or any other approval requirements, or notice requirements (such as notification to the customer of the right to restrict use of, disclosure of, and access to CPNI), contained in the FCC's regulations. We also review all notices required by the FCC regulations for compliance therewith.

7. Customer Service Managers, Kelly Wienholz or Amanda Singleton, Marketing & Commercial Sales Manager, Debbie Reding or I also ensure that the Company enters into confidentiality agreements, as necessary, with any joint venture partners or independent contractors to whom it discloses or provides access to CPNI.

Notice to Customer of Account Changes

1. The Company must notify the Customer immediately by either mail to the address of record, or by voicemail or text message to the telephone number of record upon the following events:
 - a. A new password is created or changed.
 - b. The address of record is changed.
 - c. The on-line account of record is changed.
 - d. Back-up questions are used to re-issue a lost or forgotten password.
 - e. A security breach occurs.

**CERTIFICATE OF COMPLIANCE WITH PROTECTION OF
CUSTOMER PROPRIETARY NETWORK INFORMATION RULES (Cont.)**

Reporting of CPNI Violations and Breaches

The following represents a CPNI violation or breach:

1. Customer account information is stolen,
2. CDRs are provided without authentication,
3. A pretext is attempted, or
4. Databases are hacked.

Company employees, agents and independent contractors are required to report a violation or breach to the Company Compliance Officer immediately upon knowledge of such violation or breach.

The Company shall notify law enforcement of a breach of its customers' CPNI no later than seven business days after a reasonable determination of a breach through a central reporting facility to the United States Secret Service (USSS) and the Federal Bureau of Investigation (FBI). The Company may notify the Customer and/or disclose the breach publicly after seven days following the notification to the USSS and FBI. The Customer notification timeline may be revised at the request of law enforcement.

Distribution of CPNI to Law Enforcement Agencies / FCC Notification

1. In the absence of an appropriate written request from the customer, the Company will provide the Customer's phone records or other CPNI to a law enforcement agency only in response to a warrant or subpoena that specifies the particular CPNI to be furnished. Company employees must direct all requests of CPNI from law enforcement agencies (whether or not the request is accompanied by a warrant or subpoena) to the CPNI Compliance Officer, who will be responsible for handling such requests.
2. The Company will provide written notice within five (5) business days to the FCC of any significant instance where Opt-out mechanisms do not work effectively.

I personally oversee completing and submitting EB Docket No. 06-36, which is due on or before March 1 each year which is signed and certified by Company President & CEO, Brian Haynes. The form includes explanation of any action taken against data brokers, a summary of all customer complaints, and an explanation of breaches.



Signature

Mashell Telecom, Inc. d/b/a Rainier Connect
Company

02/28/11
Date