DOCKET FILE COPY ORIGINAL

ROOTED HERE. **REACHING THERE.**

RELIANCE CONNECTS

P.O. Box 189
Estacada, OR 97023
PHONE (503) 630-4202
www.relianceconnects.com

Your local source for voice · video · broadband
A division of Cascade Utilities · CCB# 121846

January 28, 2014

Received & Inspected

FEB 04 2014

FCC Mail Room

Marlene H. Dortch, Secretary
Office of the Secretary
Federal Communications Commission
445 12th Street S.W. Suite TW-A325
Washington, D.C. 20554

RE: Certification of CPNI Filing January 28, 2014

Dear Secretary Dortch:

In accordance with 47 CFR 64.2009(e), I Brenda Crosby, President, hereby certify that for the year 2013 I have personal knowledge that Trans Cascades Telephone Company d/b/a Reliance Connects has established operating procedures, as described in the attached documentation, that are adequate to ensure compliance with the FCC's CPNI rules (47 CFR 64.2001 et seq.).

I hereby certify that the information contained in this certificate and the attached documentation is accurate and complete to the best of my knowledge, information and belief.

Sincerely,

Brenda Crosby

Brenda Crosby

NAME: Brenda Crosby
TITLE: President

No. of Copies rec'd 0+4
List ABCDE

Received & Inspected

FEB 04 2014

FCC Mail Room

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

# EB Docket 06-36

Annual 64.2009(e) CPNI Certification for 2014 covering the prior calendar year 2013

1. Date filed: January 28, 2014

2. Name of company(s) covered by this certification: Trans-Cascades Telephone Company d/b/a Reliance Connects

3. Form 499 Filer ID: 805350

4. Name of signatory: Brenda Crosby

5. Title of signatory: President

I, Brenda Crosby, 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 Brenda Crosby

**Attachments:** Accompanying Statement explaining CPNI procedure

# CPNI Usage Policy Statement

Pursuant to Section 64.2009(e) of the Federal Communication's rules, this statement explains how Trans-Cascades Telephone Company d/b/a Reliance Connects operating procedures ensure compliance with Part 64, Subpart U, of the FCC's rules.

## Company Usage of CPNI

The company has CPNI procedures that set forth the company's CPNI policies and outline what CPNI is and when it may or may not be used without customer approval by the company.

The company's procedures set forth that the use of CPNI for the purpose of marketing a service to which a customer does not already subscribe is prohibited without prior customer notice and approval. The company will not provide any affiliate, CPNI of any customer who does not also subscribe to the services provided by that affiliate, without prior customer notice and approval.

The company's procedures clearly set forth when CPNI may be used without customer approval. The company's procedures provide that the company may use CPNI to protect it's rights and property, customers, and other carriers from fraudulent, abusive or unlawful use of, or subscription to company's services.

## The Company's Notice and Approval Procedures

The company's procedures set forth the manner in which the company obtains approval from customers for the use of CPNI and weather such approval must be obtained through written, oral or electronic methods. The company's procedures set forth the period of time when such approval or disapproval to use CPNI remains in effect and the point in time when such approval is limited or revoked.

The company's procedures require that the company maintain records of customer approval, weather oral, written or electronic for at least 1 year.

The company's procedures set forth the procedures required to provide notification to customers prior to any solicitation for customer approval and the company's right to use a customers CPNI. Such procedures require the company to provide a "Notice" to a customer explaining that the customer has a right, and the company has a duty, under federal law to protect the confidentiality of CPNI. The notice must explain to the customer that the customer may restrict the use of, disclosure of, and access to its CPNI. The company maintains record of all such notifications for at least 1 year.

The Company's procedures require that any customer notification provide information sufficient to enable a customer to make an informed decision as to whether to permit the company to use it's CPNI. At a minimum, the notification must include a definition of CPNI and description of the purposes for which CPNI will be used, and inform the customer of his or her right to disapprove those uses and deny or withdraw access to the CPNI at any time. The notification must advise the customer of the precise steps the customer must take to grant or deny access to

CPNI, and state that a denial of approval will not affect the provision of any services to which the customer subscribes. The company's notification must be proximate to any solicitation for the use of CPNI.

The company's CPNI procedures set forth the use of opt-out approvals, and outline all FCC requirements regarding methods of delivery, timing of response and content requirements.

**Company's CPNI Safeguards**

The company has implemented a system by which the status of a customers CPNI approval can be clearly established prior to the use of CPNI.

The company has established the procedures for training of its personnel. Employees have been trained as to when they are and are not authorized to use CPNI. The company's CPNI procedures describe the disciplinary process related to non compliance with CPNI obligations. Refresher training courses are often scheduled.

The company's CPNI procedures and or employee manuals contain express disciplinary procedures applicable to employees who violate company policies, including CPNI policies, which can include termination of employment.

The company maintains a written record of its sales and marketing campaigns that use CPNI, including a description of each campaign, the specific CPNI that was used in the campaign, the date a purpose of the campaign and specific products and services offered as part of the campaign. The company maintains these records for a period of at least one year.

The Company has established a supervisory review process regarding Company compliance with the FCC's CPNI rules. The Company's supervisory process ensures compliance with the FCC's rules on outbound marketing situations, and the Company maintains records of compliance with these rules for a period of at least one year. The Company's procedures require that all sales personnel obtain supervisory approval of any proposed outbound marketing request.

The Company has appointed a corporate officer that has been named as the CPNI Compliance Officer and is held responsible for annually certifying that the Company is in compliance with the FCC's CPNI rules and submitting such certification and accompanying statement of how the company complies with the FCC's CPNI rules to the FCC by March 1.

The Company takes reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI. Company authenticates a customer prior to disclosing CPNI based on customer initiated telephone contact, online account access, or an in-store visit.

The Company only discloses call detail information over the telephone, based on customer-initiated telephone contact, if the customer first provides a password that is not prompted by the carrier asking for readily available biographical information or account information. If a customer does not provide a password, Company only discloses call detail information by sending it to an address of record or by calling the customer at the telephone of record. If the

customer is able to provide call detail information during a customer initiated call without Company's assistance, then Company is permitted to discuss the call detail information provided by the customer.

For accounts that are password protected, Company cannot obtain the password by asking for readily available biographical information or account information to prompt the customer for his password. A customer may also access call detail information by establishing an online account or by visiting a carrier's retail location. If a password is forgotten or lost, Company uses a back-up customer authentication method that is not based on readily available biographical information or account information. If a customer does not want to establish a password, the customer may still access call detail based on a customer-initiated telephone call, by asking Company to send the call detail information to an address of record or by the carrier calling the telephone number of record.

If a customer is able to provide to the Company, during a customer-initiated telephone call, all of the call detail information necessary to address a customer service issue (i.e., the telephone number called, when it was called, and if applicable, the amount charged for the call) then Company proceeds with its routing customer carrier procedures. Under these circumstances, Company may not disclose to the customer any call detail information about the customer account other than the call detail information that the customer provides without the customer first providing a password.

The Company password-protects online access to all CPNI, call detail and non-call detail.

The Company may provide customers with access to CPNI at a carrier' location if the customer presents a valid photo ID and the valid photo ID matches the name on the account.

The Company notifies a customer immediately when a password, customer response to a back-up means of authentication for lost or forgotten passwords, online account, or address of record is created or changed through a carrier-originated voicemail or text message to the telephone number of record, or by mail to the address of record.

In the event of a CPNI breach, Company delays customer notification of breaches until law enforcement has been notified of a CPNI breach. Company will notify law enforcement of a breach of its customers' CPNI within seven business days after making a reasonable determination of a breach by sending electronic notification through a central reporting facility to the United States Secret Service (USSS) and the FBI. If the relevant investigating agency determines that public disclosure or notice to customers would impede or compromise an ongoing or potential criminal investigation or national security, that agency may direct Company not to disclose the breach for an initial 30-day period. The law enforcement agency must provide in writing to the carrier its initial direction and any subsequent direction.

The Company, however, may immediately notify a customer or disclose the breach publicly after consultation with the relevant investigative agency, if Company believes there is an extraordinarily urgent need to notify a customer or class of customers to avoid immediate and irreparable harm.

The Company maintains a record of any discovered breaches and notifications to the USSS and the FBI regarding those breaches, as well as the USSS and the FBI response to the notifications for a period of at least two years.