NORTH STATE

February 18, 2016

**FILED ELECTRONICALLY VIA ECFS**

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

**Re: CPNI Compliance Certification and Accompanying Statement**
**EB Docket No. 06-36**
**North State Telephone Company d.b.a. North State Communications**

Dear Ms. Dortch:

In accordance with Section 64.2009(e) of the Commission's rules, North State Telephone Company d.b.a. North State Communications (Form 499 Filer ID: 806706) hereby submits its CPNI Certification and Accompanying Statement for 2016 covering the prior calendar year 2015. If you have questions or require additional information, please call me at (336) 886-3801 or email andrew.stevenson@nscom.com.

Sincerely,

Andrew Stevenson
External Affairs Analyst

Enclosure

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

**NORTH STATE TELEPHONE COMPANY d.b.a. NORTH STATE COMMUNICATIONS**

**P. O. Box 2326, High Point, NC 27261**

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

**EB Docket No. 06-36**

Annual 64.2009(e) CPNI Certification for 2016 covering the prior calendar year 2015.

1. Date Filed: February 18, 2016

2. Name of Company Covered by this Certification: North State Telephone Company d.b.a. North State Communications

3. Form 499 Filer ID: 806706

4. Name of signatory: Lynn B. Welborn

5. Title of signatory: Vice President & CAO

6. Certification:

I, Lynn B. Welborn, certify that I am an officer of the company named above ("Company"), 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, safeguards, recordkeeping, and supervisory review) set forth in Section 64.2001, *et seq.* of the Commission's rules.

The Company has not taken any 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 during 2015 or related to 2015.

The Company has not received customer complaints during 2015 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: Lynn B. Welborn Date: 2-17-16

**Attachments**: Accompanying statement explaining CPNI procedures

## NORTH STATE TELEPHONE COMPANY d.b.a. NORTH STATE COMMUNICATIONS

**P.O. Box 2326, High Point, NC 27271**

### STATEMENT OF OPERATIONAL COMPLIANCE WITH THE COMMISSION'S CPNI RULES

In accordance with Section 64.2009(e) of the Commission's rules, this accompanying statement explains how the operating procedures established by North State Telephone Company d.b.a. North State Communications ("North State" or "Company") ensure that the Company is in compliance with the requirements set forth in Section 64.2001 *et seq.* of the Commission's rules, governing the use and disclosure of Customer Proprietary Network Information ("CPNI"). North State's compliance with the Commission's CPNI rules is demonstrated by the policies, practices, and training procedures detailed below.

**Section 64.2005. Use of customer proprietary network information without customer approval.**

Although the Company does not use CPNI for marketing service offerings, the Company's CPNI policies ensure that, absent customer approval, CPNI would only be used for the purpose of providing or marketing service offerings among the categories of service to which the customer already subscribes. The Company's CPNI policies prohibit the sharing of CPNI among affiliated companies, except as permitted under Rule 64.2005(a)(1) or with customer approval pursuant to Rule 64.2007(b). The only exceptions to these policies are as permitted under 47 U.S.C. § 222(d) and Rule 64.2005.

**Section 64.2007. Approval required for use of customer proprietary information.**

In all circumstances where customer approval is required to use, disclose, or permit access to CPNI, the Company's CPNI policies require that customer approval be obtained through written, oral or electronic methods in accordance with Rule 64.2007. A customer's approval or disapproval to use, disclose, or permit access to his/her CPNI remains in effect until the customer revokes or limits such approval or disapproval. The Company maintains records of approval, whether oral, written or electronic, for at least one year.

The Company does not use CPNI for marketing communications-related services and does not disclose or grant access to CPNI to agents or affiliates that provide communication-related services, except as permitted under 47 U.S.C. 222(d) and Rule 64.2005.

**Section 64.2008. Notice required for use of customer proprietary network information.**

Prior to any solicitation for customer approval to use, disclose, or permit access to a customer's CPNI, the Company provides a customer notice of the customer's right to restrict use of, disclosure of, and access to his/her CPNI. Such customer notices, whether written, oral or electronic, are compliant with Rule 64.2008. The Company maintains records of such customer notices for a minimum of one year.

The Company does not currently solicit "opt out" customer approval to use, disclose, or permit access to CPNI because the Company does not use a customer's individually identifiable CPNI for the purpose of marketing communications-related services to that customer. The Company does not

disclose or permit access to a customer's individually identifiable CPNI to agents or affiliates for the purpose of marketing communications-related services, except as permitted under 47 U.S.C. 222(d) and Rule 64.2005.

The Company does not currently solicit "opt in" customer approval to use, disclose, or permit access to a customer's individually identifiable CPNI because the Company does not use, disclose, or permit access to a customer's individually identifiable CPNI in any manner that would require a customer's "opt in" approval under the Commission's CPNI rules, except as permitted under 47 U.S.C. 222(d) and Rule 64.2005.

The Company's CPNI policies include employee training on the customer notice and customer approval requirements specific to limited, one-time use of CPNI for marketing purposes. In all instances where the Company seeks customer approval to obtain one-time use of CPNI for inbound and outbound customer telephone contacts for the duration of the call, the Company obtains such approval in accordance with Rule 64.2008(f).

**Section 64.2009. Safeguards required for use of customer proprietary network information.**

The Company's CPNI policies include employee training on the restrictions on the use and disclosure of CPNI. The Company's billing and provisioning system allows authorized Company personnel to clearly establish the status of a customer's CPNI approval prior to the use of CPNI. The Company has established an express disciplinary process to address unauthorized use or disclosure of CPNI by its employees.

Although the Company and its affiliates do not use CPNI for sales or marketing purposes, nor disclose or permit access to CPNI to third parties, the Company's CPNI policies require the Company to maintain a record of the sales and marketing campaigns that use CPNI and all instances where CPNI was disclosed to third parties, or where third parties were permitted access to CPNI. Such records are maintained for a minimum of one year and include the required information listed under Rule 64.2009(c).

The Company has established a supervisory review process regarding the Company's compliance with the Commission's rules covering the use of CPNI in outbound marketing campaigns. The Company maintains records of its compliance with the Commission's CPNI rules for a minimum of one year. Although the Company does not use CPNI for marketing purposes, the Company's CPNI policies require sales personnel to obtain approval from the Company's CPNI Compliance Officer of any proposed outbound marketing campaign that uses CPNI. Record of the marketing campaign and the appropriate supervisory approval is maintained for a minimum of one year.

The required officer certification, statement of actions taken by the Company against data brokers, and summary of customer complaints pertaining to the unauthorized release of CPNI are included with this accompanying statement. The Company will file these documents on an annual basis on or before March 1, for data pertaining to the previous calendar year.

The Company's CPNI policies require the Company to provide written notice to the Commission within five business days of any instance where the opt-out mechanism does not work properly, to such

a degree that customers' inability to opt-out is more than an anomaly. Such notices are compliant with Rule 64.2009(f).

**Section 64.2010. Safeguards on the disclosure of customer proprietary network information.**

The Company's CPNI policies and employee training include reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI, a practice known as pretexting. Employees are trained to properly authenticate a customer prior to disclosing CPNI based on customer-initiated telephone contact, online account access, or an in-store visit. Employees are instructed to notify the CPNI Compliance Officer of any suspected pretexting.

The Company's CPNI policies ensure that call detail information may only be disclosed if the customer first provides the Company with a password that is not prompted by Company asking for readily available biographical or account information. If the customer does not provide a password, the Company may only disclose call detail information by sending it to the customer's address of record, by calling the customer at the telephone number of record, or if the customer is able to provide call detail information to the Company during a customer-initiated call without the Company's assistance.

The Company's CPNI policies require customer authentication without the use of readily available biographical or account information, prior to allowing the customer online access to CPNI. Once the customer is authenticated, the customer may only obtain access to his/her online account through a password. The Company's policies covering the establishment of a password for an online account and a back-up authentication method for lost or forgotten passwords are compliant with Rule 64.2009(e).

The Company's CPNI policies permit the disclosure of CPNI to a customer who, at one of the Company's retail offices, first presents the Company with a valid photo ID matching the customer's account information.

The Company promptly notifies customers whenever 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. The content of the customer notice is compliant with Rule 64.2010(f); notices are delivered by mail to the address of record and do not reveal the changed information. In the case of a change of address, customer notices are delivered by mail to the customer's former address.

**Section 64.2011. Notification of customer proprietary network information security breaches.**

The Company has established specific policies and procedures to comply with Rule 64.2011 for notifying law enforcement of a breach of its customers' CPNI. When it is reasonably determined that a breach has occurred, the Company's CPNI Compliance Officer will notify law enforcement and affected customers within the required timeframes. The Company maintains a record of any breaches discovered, including notifications made to law enforcement and to customers, for a minimum of two years.