



NORTHEAST RURAL SERVICES, INC.
A subsidiary of Northeast Oklahoma Electric Cooperative, Inc.
Mailing Address: PO Box 399, Vinita, OK 74301-0399
Physical Address: 27039 South 4440 Road, Suite B, Vinita, OK
Office: 918-256-9333 Facsimile: 918-256-9311
This institution is an equal opportunity employer and provider.

February 27, 2019

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

DOCKET FILE COPY ORIGINAL

Received & Inspected

MAR 01 2019

FCC Mailroom

Re: EB Docket No. 06-36
Annual 47 CFR 64.2009(e) CPNI Certification
NORTHEAST RURAL SERVICES, INC.
Form 499 Filer ID Number(s): 831079
Which also includes: d/b/a BOLT Fiber Optic Services

Dear Secretary Dortch,

In accordance with 47 CFR 64.2009(e), please find attached company's Annual CPNI Certification for the previous calendar year, 2018. The Certification includes the company's:

- Statement explaining how its operating procedures ensure compliance with 47 C.F.R., Part 64, Subpart U;
- An explanation of any actions taken against data brokers; and
- A summary of all customer complaints received in the past year concerning the unauthorized release of customer proprietary network information (CPNI).

If you have any questions regarding this filing, please direct them to the undersigned.

Sincerely,

Daniel Webster
General Manager/CEO

Attachment

No. of Copies rec'd
List ABCDE

0+4

ANNUAL 47 C.F.R. § 64.2009(e) CPNI Certification
EB Docket 06-36

Annual 64.2009(e) CPNI Certification for 2019 covering the prior calendar year 2018.

1. Date Filed: February 27, 2019
2. Name of company covered by this certification: Northeast Rural Services, Inc.
Name filer is doing business as: BOLT Fiber Optic Services
3. Form 499 Filer: 831079
4. Name of Signatory: Daniel Webster
5. Title of signatory: General Manager
6. Certification:

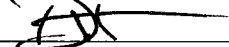
I, Daniel Webster, certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's rules. *See* 47 C.F.R. § 64.2001 *et seq.*

Attached to this verification 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 action (*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 to enforcement action.

Signed:  _____

Attachments: Accompanying Statement explaining CPNI procedures.

Summary of CPNI Compliance Manual and Operating Procedures of Northeast Rural Services, Inc. (NRS)

The following summary describes provisions of NRS's CPNI Compliance Manual and Operating Procedures (Policy). NRS's procedures are 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 U.S.C. § 222, and the FCC's regulations, 47 C.F.R., Part 64, Subpart U. The Policy protects the confidentiality of CPNI and relies on the involvement of high-level management to ensure that no use of CPNI is made until legally compliant. The Policy is administered by NRS's General Manager, Daniel Webster, and Manager of Information Technology, Ricky Hignite. NRS maintains the Policy in its offices for purposes of training employees and as a reference guide for all CPNI issues. Summarily:

I. CPNI USE, DISCLOSURE, ACCESS

NRS has a duty to protect the confidentiality of its Customers' CPNI. NRS must disclose CPNI, upon affirmative written request by the Customer, to any person designated by the Customer. When NRS receives or obtains CPNI by virtue of its provision of a Telecommunications Service, it can only use, disclose, or permit access to individually identifiable CPNI in its provision of the Telecommunications Service from which the information is derived; or Services necessary to, or used in, the provision of the Telecommunications Service. When NRS receives or obtains CPNI from another Carrier for purposes of providing any Telecommunications Service, it shall use such CPNI only for such purpose, and not for its own marketing efforts. NRS cannot use, disclose or permit access to CPNI to identify or track Customers that call competing service providers. NRS may use, disclose, or permit access to CPNI to provide inside wiring installation, maintenance, and repair services, for the provision of CPE and call answering, voice mail or messaging, voice storage and retrieval services, fax store and forward, and protocol conversion; to protect the rights or property of NRS, or to protect users of services and other Carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services; to initiate, render, bill and collect for Telecommunications Services, or as otherwise provided by law. NRS does not currently use CPNI to market service offerings among the different categories of service, or even within the same category of service, that it provides to subscribers.

II. NRS SAFEGUARDS AND RECORDKEEPING REQUIREMENTS

NRS must take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI. NRS must properly authenticate a Customer prior to disclosing CPNI based on Customer-initiated telephone contact, online account access, or an in-person visit. NRS will only disclose Call Detail Information over the telephone, based on Customer-initiated telephone contact, if the Customer first provides the Carrier with a password that is not prompted by the NRS asking for Readily Available Biographical Information, or Account Information. If the Customer does not provide a password, or does not wish to create a password, NRS may only disclose Call Detail Information by sending it to the Customer's Address of Record, or, by calling the Customer at the Telephone Number of Record (rather than using Caller ID). NRS must authenticate a Customer without the use of Readily Available

Biographical Information, or Account Information, prior to allowing the Customer online access to CPNI related to a Telecommunications Service account. NRS may disclose CPNI to a Customer who, in NRS's office, first presents a Valid Photo ID (a government-issued means of personal identification with a photograph such as a driver's license, passport, or comparable identification that is not expired) matching the Customer's Account Information and the person is listed on the account.

NRS 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. NRS personnel make no decisions regarding CPNI without first consulting with management. All compliance matters and any violation of, or departure from, the policies and procedures in this Policy shall be reported immediately to Daniel Webster, General Manager and Ricky Hignite, Manager of Information Technology. Any improper use of CPNI will result in appropriate disciplinary action in accordance with established NRS disciplinary policies. Any improper use shall be treated as a serious offense, and may result in suspension or termination of employment in appropriate cases. Any NRS personnel making improper use of CPNI will undergo additional training to ensure future compliance.

NRS must notify a Customer immediately 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. This notification is not required when the Customer initiates service, including the selection of a password at service initiation. This notification may be through a NRS-originated voicemail or text message to the Telephone Number of Record (not caller ID), or by mail to the Address of Record, and must not reveal the changed information or be sent to the new Account Information. A change of address shall be mailed to the former address, rather than the new address.

The authentication requirements for disclosure of CPNI do not apply to disclosure of business customer information by a dedicated account representative who knows through personal experience that the person requesting the information is an authorized representative of the customer and that the contract between NRS and that business customer specifically addresses the protection of CPNI.

NRS must maintain a record, electronically or in some other manner, of any Breaches discovered, notifications made to the United States Secret Service (USSS) and the Federal Bureau of Investigation (FBI) pursuant to the above paragraphs, and notifications made to Customers. The record must include, if available, dates of discovery and notification, a detailed description of the CPNI that was the subject of the Breach, and the circumstances of the Breach. NRS must retain the record for a minimum of two (2) years.

III. REPORTING BREACHES

NRS will take reasonable steps to protect CPNI databases from hackers and other unauthorized attempts by third parties to access CPNI. NRS must notify law enforcement of a Breach of its Customers' CPNI. A Breach occurs when a person, without authorization or exceeding authorization, has intentionally gained access to, used, or disclosed CPNI. NRS shall not notify

its Customers or disclose the Breach publicly, whether voluntarily or under state or local law or these rules, until it has completed the process of notifying law enforcement. As soon as practicable, and in no event later than seven (7) business days, after reasonable determination of the Breach, NRS shall electronically notify the USSS and the FBI through a central reporting facility. The Commission will maintain a link to the reporting facility at <http://www.fcc.gov/eb/cpni>. NRS will indicate its desire to notify its Customer or class of Customers immediately concurrent with its notice to the USSS and 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, such agency may direct NRS not to so disclose or notify for an initial period of up to 30 days. Such period may be extended by the agency as reasonably necessary in the judgment of the agency. If such direction is given, the agency shall notify NRS when it appears that public disclosure or notice to affected Customers will no longer impede or compromise a criminal investigation or national security. After NRS has completed the process of notifying law enforcement, it shall notify Customers of the Breach. All breach reporting shall comply with 42 C.F.R. § 64.2011.

IV. TRAINING

All NRS employees with access to CPNI receive training and a copy of NRS' CPNI policies. The training includes emphasis that violations of its CPNI policies will result in disciplinary action, including the termination of employment where appropriate, and also that employees may be subject to criminal penalties if they knowingly facilitate the unauthorized disclosure of a customer's confidential information.