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

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

1. Date filed: 02/16/18

2. Name of company covered by this certification: Rural Telephone Service Company, Inc. d/b/a Nex-Tech

3. Form 499 Filer ID: 804438

4. Name of signatory: Rhonda S. Goddard

5. Title of signatory: Chief Financial Officer

6. Certification:

I, Rhonda S. Goddard, 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, safeguards, 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, with 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: 

Attachments: Accompanying Statement explaining CPNI procedures

9.3 Customer Proprietary Network Information (CPNI)

This procedure is intended to ensure compliance with the Federal Communications Commission's (FCC) CPNI rules (47 CFR 64.2001.-64.20011) and will govern the process of handling customer requests to restrict or allow use of CPNI. The CPNI statement will be reviewed annually with all employees. The Director of Customer Engagement (DCE) will be responsible for submitting annual FCC compliance filings and will certify training programs.
The CFO is the Compliance Officer acting as an agent for the Company.

Customer Notification:
The Company will notify and inform each Customer of his/her right to restrict the use or disclosure of and access to CPNI along with a solicitation of opt-out approval every other year.

The Company will maintain records of that notification in the current billing software, whether oral or written, for at least one (1) year. The notification will:

1. Provide information sufficient to enable customers to make informed decisions as to permit the use or disclosure of or access to their CPNI,
2. Contain a statement that the customer has a right, and the Company has a duty under federal law to protect the confidentiality of CPNI, and
3. Specify the types of information that constitute CPNI and the specific entities that will receive CPNI, describe the purposes for which CPNI will be used, and inform the customer of his/her right to disapprove those uses and deny or withdraw access for use of CPNI at any time. Any approval or withdrawal will remain in effect until the customer revokes or limits the approval or denial.

Through "opt-out" approval, a customer is deemed to have consented to the use of the customer's CPNI if the customer has failed to object within the thirty-day (30) period identified in the notice. The thirty-day (30) clock begins three (3) days following the mailing date of the notification.

Through "opt-in" approval, the customer provides express consent allowing CPNI usage, disclosure, or access.

The Company may allow one (1) time use of CPNI through verbal customer authorization to obtain limited use of CPNI for in-bound or out-bound customer telephone contacts for the duration of that call.

The Company will advise the customer of the precise steps the customer must take in order to grant or deny access to CPNI, and the Company will clearly state that a denial of approval will not affect the provision of any services the customer has.

The notification will be in a clear and neutral language which describes the consequences directly resulting from the lack of access to CPNI. In addition, the Company may state that the customer's consent to use his/her CPNI may enhance the Company's ability to offer products and services tailored to meet the customer's needs, and the Company will disclose the customer's CPNI to any person upon the affirmative written request of the customer. The notification will not include any statement that attempts to encourage a customer to freeze third-party access to CPNI.

New customers will be verbally notified of CPNI procedures at the time of the request for service. In addition, a CPNI statement will be included in the new customer welcome packet.

CPNI Use:
The Company may use, disclose, or permit access to CPNI to protect Company rights, property, customers, and other carriers from fraudulent, abusive, or unlawful use of or subscription to Company services.

The Company may use, disclose, or permit access to CPNI to provide or market service offerings among the different categories of service: local, inter-exchange, VoIP, video services, Internet, etc. to which the customer already subscribes.

When the Company provides different categories of service(s), and a customer subscribes to more than one (1) service category, employees can share the customer's CPNI with the affiliate that provides service to the customer; however, if a customer subscribes to only one (1) offering, employees should not share the customer's CPNI with an affiliate without the customer's express approval.

Without customer approval, employees will not use, disclose, or permit access to CPNI to provide or market service offerings within a category of service to which the customer does not already subscribe except to use, disclose, or permit access to CPNI to do the following:

1. Provide inside wiring installation, maintenance, repair services, and provision of customer premise equipment (CPE), and
2. Provide services, such as, but not limited to: voice mail or messaging, voice storage and retrieval, protocol conversion speed dialing, computer-provided directory assistance, call monitoring, call tracing, call blocking, call return, call tracking, call waiting, caller ID, call forwarding, and some Centrex features.

CPNI Approvals:

The Company will honor a customer's approval or withdrawal until the customer revokes or limits the approval or withdrawal. If the Company discloses or allows access to customers' individually identifiable CPNI to an affiliate, the Company will require the affiliate to enter into a confidential agreement in order to safeguard information requiring that:

1. The affiliate's use of CPNI is only for the purpose of marketing or providing the communications-related services for which CPNI has been provided,
2. The affiliate will not permit any other party to use, allow access to, or disclose the CPNI to any other party, unless they are required to make disclosure under force of law, and
3. The affiliate will have appropriate protections in place to ensure the ongoing confidentiality of CPNI.

Customer Authentication for Call Detail:

Since the release of call detail information over the telephone presents an immediate risk to privacy, the Company is prohibited from releasing call detail information based on customer-initiated telephone contact, except under three (3) circumstances:

1. When a customer provides a pre-established password,
2. When a customer requests the information be sent to the address of record, or
3. When a representative of the Company calls the telephone number of record and discloses the information to an authorized contact.

At retail locations, staff may continue to provide account access to customers who present valid photo IDs as the authorized contact.

Password protection is not required for routine customer care procedures regarding service/billing disputes or questions if the customer is able to provide all of the call detail information necessary to address the customer question, i.e., telephone number called, when it was called, and amount charged for the call. In addition, the Company will provide mandatory password protection for online account access. Online access based solely on a customer's readily available biographical information is prohibited.

Establishing a Password:

For existing customers, staff must first authenticate the customer by either calling the account number on record or requesting that the customer present a valid photo ID in person at any retail location.

For a new customer, the Company may establish a password at the time of service initiation, and the customer may be authenticated at that time.

Customer Account Authentication:
The Company will authenticate the customer by telephone for their protection and confirm the person is the account holder by requesting authentication which may include, but is not limited to the following: year of birth of primary account holder, last four (4) digits of the primary account holder's driver's license number, account number of the primary holder's Nex-Tech account, or last four (4) digits of the primary account holder's social security number.

Authentication information will be acquired from new customers at the time of request for service or obtained on the appropriate form through the mail.

The Company will not discuss the following account information with a spouse, child, parent, etc., unless they are authorized by the account holder. Account information may include, but is not limited to: name, address, phone number, ESN, billings or charges, balance due or payment status, text messages, or data services.

A maximum of four (4) authorized contacts may be added to the account by the authorized account holder.

All printed documents, notes, and materials with customer information will be shredded and disposed of properly. This may include, but is not limited to: customer's social security number, name, address, phone number, or a copy of bill or remittance slip.

Law Enforcement:
All court-ordered requests or subpoenas for customer account or billing information will be directed to the appropriate staff member as outlined in Section 12.6, Subpoenas for Company Information, based on the data requested.

Notice of Account Changes:
The Company must notify a customer immediately of account activity, such as a change to a password, online account, or address of record. Notification may be sent by email, voicemail, text message, or US Mail to the customer's address of record.

Notice of Unauthorized Disclosure of CPNI:
The DCE will be notified of any potential unauthorized disclosure of CPNI, and it will be investigated to determine if an actual breach has occurred.

In the case of a breach of CPNI, the DCE will provide electronic notification of the breach within seven (7) business days to the United States Secret Service (USSS) and the Federal Bureau of Investigation (FBI). The FCC link to report breaches is www.fcc.gov/eb/CPNI/. In order to allow law enforcement time to conduct an investigation, the Company must wait a minimum of seven business (7) days before notifying the affected customers of the breach, unless the USSS and FBI request that the carrier continue to postpone disclosure. However, if authorized by the authorities, the Company may notify customers sooner if there is a risk of immediate and irreparable harm. In addition, the Company must keep records of discovered breaches for at least two (2) years.

Joint Venture and Independent Contractor Use of CPNI:
The Company must obtain opt-in consent from a customer before disclosing a customer's CPNI to a joint venture partner or an independent contractor to market communication services to the customer.

Business Customers:
The Company may establish authentication procedures for business customers that are different from residential customers, as long as those customers have a dedicated account representative and the service contracts specifically address the protection of CPNI.

CPNI Compliance:
The Company has implemented a system by which the status of a customer's CPNI approval can be clearly established prior to the use of the CPNI.

All employees will sign a CPNI Procedure Acknowledgement that will be placed in their personnel file.

All employees with access to CPNI will be trained and certified. To become certified, the employee will receive and read the company's CPNI procedure, and attend group or individual training certified by the DCE. The training will provide explicit details as to when employees are, and are not, authorized to disclose CPNI.

For unintentional violations breaching CPNI, employees may be reprimanded, retrained, and recertified. For repeated unintentional violations, employees may be disciplined or terminated. In most cases, the unintentional violations will not be considered a breach of CPNI procedures.

For intentional violations, such as distribution of CPNI to third parties for financial gain, or to harm the Company or customer, the breach must be reported, and the employee will be terminated.

The DCE will maintain a record of the Company and affiliate sales and marketing campaigns that use customer CPNI. The record includes a description of each campaign, the specific CPNI that was used in the campaign, and what products and services were offered as part of the campaign. These records will be retained for at least one (1) year.

The Company has established a supervisory review process regarding compliance with CPNI rules for outbound marketing promotions and maintains compliance records for at least one (1) year. Specifically, Company sales personnel will obtain supervisory approval of any proposed outbound marketing request and customer approval of the use of CPNI.

The Company will provide written notice within five (5) business days to the FCC of any instance where the "opt-out" mechanisms do not work properly to a degree that consumers' inability to "opt-out" is more than an anomaly. The notice will be in the form of a letter and include the Company's name, a description of the opt-out mechanism(s) used, the problem(s) experienced, the remedy proposed and when it will be/was implemented, whether the Kansas Corporation Commission (KCC) has been notified and if it has taken any action, a copy of the notice provided to customers, and contact information. This notice must be submitted even if the Company offers other methods by which customers may "opt-out."