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

EB Docket 06-36

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

1. Date filed: February 15, 2019
2. Name of company(s) covered by this certification: Community Fiber Solutions
3. Form 499 Filer ID 828803
4. Name of signatory: Roger J Criblez
5. Title of signatory: Asst to CEO / Acting CFO]
6. Certification:

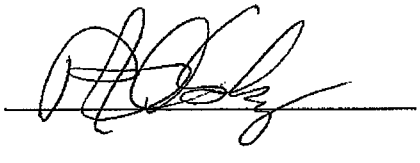
I, Roger J Criblez, certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. *See* 47 C.F.R. § 64.2001 *et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

Attachments: Accompanying Statement explaining CPNI procedures

BENTON RIDGE TELEPHONE COMPANY

WATCH TV COMPANY

COMMUNITY FIBER SOLUTIONS, INC.

BRIGHT.NET-BRT, INC.

CUSTOMER PROPRIETARY NETWORK INFORMATION

(CPNI)

POLICY HANDBOOK

INTRODUCTION

This handbook contains the policies and procedures of Benton Ridge Telephone Company, WATCH TV Company, Community Fiber Solutions, Inc., Bright.net-BRT, Inc., and any other affiliates classified by the FCC as telecommunications carriers, broadband providers, or interconnected VOIP providers (collectively referred to as "the Company") that have been put in place to protect Customer Proprietary Network Information ("CPNI"). Under federal law, all communications carriers are required to protect CPNI. The FCC has passed strict regulations that carriers must comply with to combat pretexting, which refers to the process by which data brokers pose as customers or law enforcement officials to obtain confidential customer information.

The CPNI policy of Benton Ridge Telephone Company and its affiliates extends to all broadband customers, where appropriate.

Our employees are expected to learn and follow the policies contained in this handbook. The Company is required to file a certificate stating that it is in compliance with FCC regulations every year. Without full compliance by our employees, the Company may be subject to FCC fines and other penalties. We depend on you to ensure our compliance.

If you have any questions about the policies contained in this handbook, or if you have other concerns relating to the protection of CPNI, please contact the Company's Chief Financial Officer or Corporate Secretary immediately.

CPNI POLICIES

1. What is CPNI?

CPNI is information, known to the Company solely by virtue of the carrier-customer relationship. CPNI includes:

- quality,
- technical configuration,
- type,
- destination,
- location, and
- amount of use

relating to a communications service subscribed to by any customer. This means that customer calling patterns (including phone numbers and length of calls), service plans, and equipment are CPNI.

CPNI does not include subscriber list information (*e.g.*, directory listings).

2. Duty to Protect CPNI

We as a communications company have a duty to protect customer CPNI. We may not disclose CPNI to unauthorized persons, nor may we use CPNI in certain ways without consent from our customers. Before we can provide customers with their own CPNI, we must authenticate the customer – a fancy way of saying that we must determine that customers are who they say they are before disclosing CPNI.

There are a few cases in which we can disclose CPNI without first obtaining customer approval:

a. Administrative use: We may use CPNI to *initiate, render, bill and collect* for communications services. This means that we can share CPNI with our billing vendor and billing and collection agencies.

b. Protection of carrier and third parties: We may use CPNI to protect the interests of the Company, such as to prevent fraud or illegal use of our systems and network. Employees will be notified of the steps to take, if any, in these sorts of situations.

c. As required by law: We may disclose CPNI if we are required to by law, such as through legal process (subpoenas) or in response to requests by law enforcement. Again, employees will be notified of any steps they must take in these situations.

3. Our Own Use Of CPNI

We may use CPNI to provide or market services to our existing customers. Sometimes, however, we are required to obtain customer approval prior to using CPNI in this way. For purposes of protecting CPNI, there are two different types of marketing: "total service approach" and "cross-marketing." We are required to obtain customer consent before using CPNI in cross-marketing, but not before using CPNI in the total service approach.

A. *"Total service" approach*. This means that we are marketing services to our existing customers within the categories of service to which the customer already subscribes. For instance, if we provide local telephone service to a customer, we may use the customer's local CPNI to sell other products within the local telephone service category (*e.g.*, caller ID), without first obtaining the customer's approval. Basically, the total service approach allows us to use CPNI to market additional related services and features for the customer's existing subscribed service, which may include additional or related offerings.

We do not need customer approval to use CPNI to provide customer premise equipment and call answering, voice mail or messaging, voice storage and retrieval services, fax store and forward, and protocol conversion. We also do not need customer consent before using CPNI to market "adjunct-to-basic" services such as speed dialing, computer-provided directory assistance, call monitoring, call tracing, call blocking, call return, repeat dialing, call tracking, call waiting, caller ID, call forwarding, and certain centrex features.

We cannot use CPNI to solicit a customer to add a new category of service without first obtaining the customer's approval. This is considered cross-marketing.

B. *Cross-marketing*. We may not use CPNI to market services that are in a service category to which the customer does not already subscribe without customer approval. For instance, we cannot use CPNI to market long-distance services to our local service customers without first obtaining their consent to use the CPNI.

When a customer calls, you should check the customer's account to determine whether they have previously provided us with consent to use CPNI in this manner. If they have provided us with this consent, the account will be flagged and you can proceed without seeking further approval. If they have not provided us with this consent, you should clearly state that the Company may be able to provide other services or plans based on their past and current needs, but that you need permission to look at their account history and calling patterns first. Do not proceed without obtaining the customer's consent first. You must also authenticate the customer using one of the methods outlined below (generally, by calling the customer back at the telephone number of record or having the customer provide the account password).

We will not use CPNI to identify or track customers that call competing service providers.

C. *New marketing campaigns*. We will regularly review our marketing practices to determine when and how CPNI is used within the Company, and whether CPNI is being shared with other entities. We will also review new marketing or sales campaigns to ensure compliance with these CPNI policies and with the FCC's CPNI regulations.

4. Sharing CPNI With Our Affiliates

After receiving customer consent, the Company may share CPNI with its affiliates to be used in accordance with the policies in this handbook.

5. Authenticating Customers Before Disclosing CPNI

We are required to objectively determine that our customers are who they say they are before disclosing CPNI to them. This ensures that sensitive, private information is given only to the true customers. The type of authentication required varies based on the customer's method of communicating with us: by telephone, in person, by mail, or online.

A. Telephone

When a customer calls, we may not release *call detail information*, or information relating to the transmission of specific telephone calls (numbers called, number called from, time/location/duration of any call) unless the customer provides the account password or until we have called the customer back at the telephone number of record to ensure that the customer is who s/he says s/he is.

We cannot tell customers to base their passwords on readily available biographical or account information, such as mother's maiden name, any part of their Social Security numbers, or the last four digits of the account number. However, customers are free to choose any password they would like, as long as they comply with our formatting requirements. Once the password system is in place, we may not disclose CPNI to customers over the telephone without the valid password.

If a customer has lost or forgotten his/her password, s/he must come to our office and present valid photo identification before any changes can be made to the password. However, if the customer provides a new address or telephone number at which they would like to receive the retrieved password, you should refuse and immediately contact a supervisor to notify them of a possible CPNI breach issue. We may not provide password information to a new contact address provided at the time of the password request.

If the customer cannot provide the password, we may only perform routine customer care relating to specific phone calls only if the customer is able to provide *all of the call detail information necessary to address the customer service issue* (*e.g.*, the telephone number called, when it was called, and, if applicable, the amount charged for the call). Even where a customer can provide this information, we may only disclose information relating to that specific transaction – we cannot provide other account information without proper password authentication.

Alternatively, we may offer to send the call detail information to the address of record or to the customer in person after s/he has produced valid photo identification at our offices. Details regarding these methods of communicating are below.

We may disclose *non-call detail information* (such as remaining calling plan minutes) over the telephone after authenticating the customer by calling back the telephone number of record, checking valid photo identification (when the customer is in person), or by mailing the information to the account address of record. No passwords are necessary.

B. In-Person Authentication

Before we can disclose CPNI to customers in person, the customer must present *valid government-issued photo identification* (*e.g.*, a current driver's license, passport, or comparable ID). The name on the photo identification must match the name on the account. If you have any question about

whether the identification is authentic, or if the name on the identification does not match the name on the account, you should not provide the requested CPNI.

Before providing the CPNI to the customer, make a copy of the photo identification. This copy should then be placed in the customer's file, together with a copy of the CPNI provided to the customer. These records will be kept in the customer file in accordance with our record-keeping policies outlined below.

If the customer cannot present the required identification, we will offer to provide the requested CPNI by sending it to the account address of record.

C. Mail

If the customer requests CPNI through the mail, or if the customer cannot comply with one of the authentication methods above, we will send the requested information to the customer's address of record only. This may be the billing address or the service address.

D. Online Access

We will password protect online access to CPNI, as required by the FCC. All online-access customers will establish passwords at service initiation. We will not allow customers to choose passwords based on their readily available biographical information or account data.

After a customer has made three failed attempts to log into his/her online account, we will block online access to the account for security purposes. Customers locked out of their online accounts will need to present photo identification at our office to regain online account access. Furthermore, if a customer loses or forgets his/her online account password, the customer must present photo identification at our office to obtain password information for the account.

6. Customer Notification of CPNI Rights

We will provide a CPNI privacy policy to all customers every other year. We will maintain a list of all customers who received the privacy policy, and the date on which the policy was sent, together with a copy of the policy in our records for one year following the mailing of the policy.

We will provide additional copies of the CPNI privacy policy to all customers who request it and to all new customers upon activation of service.

The policy contains an opt-out customer approval notice. Customers who do not wish to allow us to use their CPNI to market services outside their existing service categories, or who do not wish to allow the Company to share their CPNI with our affiliates, will have 30 days to contact us to tell us that they do not approve of this use. If we have not heard back from the customer within those 30 days, we will be free to use their CPNI for these purposes. Customers will be able to change their option at any time by contacting us, and we will notify our customers of this right.

We will maintain records of the customers who received the opt-out approval notice (contained within the CPNI privacy policy), and records of the customers who contacted the Company to opt out, in line with the record-keeping policies outlined below. The list of customers who received the opt-out

approval notice, but who have not contacted the Company to opt-out, will also serve as our list of customers who have provided opt-out consent to share their CPNI with our affiliates.

In accordance with the FCC's requirements, we will provide written notice to the FCC within five business days if our opt-out mechanisms do not work properly to the degree that our customers' inability to opt out is more than an anomaly. This notice will comply with the FCC's consent requirements.

7. Training And Discipline

The Company will train all employees with access to CPNI regarding our policies. These employees are required to attend an annual retraining to ensure that they understand the Company's CPNI policies and any updates to those policies. Any new employees who will have access to CPNI will be trained when they join the Company, and will then attend the regularly-scheduled retraining sessions. At the conclusion of each training session, employees will be asked to sign certificates stating that they understand the Company's CPNI policies and that they will comply with those policies.

Employees who fail to observe the Company's CPNI procedures will be subject to the disciplinary procedures contained in the Company's Handbook. Discipline may range from additional training to termination, depending on severity of the CPNI compliance failure. Records relating to this process will be maintained in the Company's files in line with the record-keeping policies outlined below.

8. Record-Keeping

The Company will maintain the following records in its files for one year:

a. Records relating to the mailing of the customer CPNI privacy policy every other year;

b. Records of customer approval or disapproval of CPNI use, or the limitation or revocation thereof;

c. Records of our own and affiliates' sales and marketing campaigns that use CPNI, all instances where CPNI was disclosed or provided to third parties, and instances where third parties were allowed access to CPNI. The records will include a description of each campaign, the specific CPNI that was used in the campaign, and what products and services were offered as a part of the campaign;

d. The Company's supervisory records, such as when sales personnel obtain supervisory approval of any outbound marketing requests for customer approval; and

e. Employee disciplinary records.

The Company will maintain records of discovered CPNI breaches, notifications to law enforcement regarding breaches, any responses from law enforcement regarding those breaches, any actions taken against data brokers, and all customer complaints concerning the unauthorized release of CPNI, in its files for two years.

9. Annual Certification Requirement

The Company will file its annual CPNI certification with the FCC on or before March 1 for data pertaining the previous year. The annual certification will contain all of the contents required by the FCC, including information regarding customer complaints, actions against data brokers, pretexting

processes encountered, and our Company procedures. An officer will sign the certification indicating that s/he has personal knowledge that the Company has established operating procedures that comply with the FCC's CPNI regulations. This officer will make any decisions regarding the redaction of confidential information in the certification.

10. Notification Of Account Changes

We will notify customers when changes have been made to passwords, customer responses to back-up means of authentication (i.e. security questions), online accounts, or addresses of record by mailing a notification to the account address of record, though we will not reveal the changed account data in the notification.

11. Unauthorized Disclosure Of CPNI

As required by the FCC, we will report CPNI breaches to law enforcement no later than seven business days after determining the breach has occurred, by sending electronic notification through the link at http://www.fcc.gov/eb/CPNI/ to the central reporting facility, which will then notify the United States Secret Service (USSS) and the Federal Bureau of Investigation (FBI). The WATCH Office Manager will be responsible for this notification.

We cannot notify customers or the public of the breach earlier than seven days after we have notified law enforcement through the central reporting facility. Before doing so, we will notify law enforcement of our desire to notify the customer. If we wish to notify customers or the public immediately, where we feel that there is "an extraordinarily urgent need to notify" to avoid "immediate and irreparable harm," we will inform law enforcement of our desire to notify and comply with law enforcement's directions.

Records relating to such notifications will be kept in accordance with the record-keeping policies outlined above. These records will include: (i) the date we discovered the breach, (ii) the date we notified law enforcement, (iii) a detailed description of the CPNI breached, and (iv) the circumstances of the breach.

During the course of the year, we will compile information regarding pretexter attempts to gain improper access to CPNI, including any breaches or attempted breaches. This will aid in the preparation of the annual compliance certification to be filed with the FCC.

* * *

These CPNI policies are an integral part of our business practices. Protecting customer confidentiality is a chief concern of our customers, and therefore a top priority for our Company.

If you have any questions regarding these policies, please notify your supervisor immediately.