



Received & Inspected

FEB 23 2010

FCC Mail Room

February 22, 2010

Marlene H. Dortch, Office of the Secretary
Federal Communication Commission
9300 East Hampton Drive
Capitol Heights, MD 20743

Dear Ms. Dortch:

Enclosed please find the City of Bristol, Virginia's, d/b/a Bristol Virginia Utilities, Customer Proprietary Network Information (CPNI) annual certification reporting.

Should you have questions or need additional information, please do not hesitate to contact me at 276.645.8707.

Sincerely,

A handwritten signature in black ink that reads "Stacey E. Bright". The signature is written in a cursive, flowing style.

Stacey E. Bright
Executive Vice President and
Chief Financial Officer

Enclosures

No. of copies rec'd. 0+4
List AEOB

15022 Lee Highway
Bristol, Virginia 24202

276-821-6100

1-866-TELE-BVU

276-821-6218

Received & Inspected

FEB 23 2010

FCC Mail Room

**ANNUAL 47 C.F.R. § 64.2009(e) OFFICER'S CERTIFICATION OF
CUSTOMER PROPRIETARY NETWORK INFORMATION (CPNI) COMPLIANCE**

EB Docket 06-36

Annual 64.2009(e) CPNI Certification for Calendar Year: 2009

Name of company covered by this certification: City of Bristol dba Bristol Virginia Utilities

Name of signatory: Brian C. Bolling

Title of signatory: Vice President of Customer Service

I, Brian C. Bolling, certify and state that:

1. I am the Vice President of Customer Service of City of Bristol dba Bristol Virginia Utilities ("BVU"), and, acting as an agent of the company, I have personal knowledge of BVU's operating procedures as they relate to CPNI, and the Rules and Regulations of the Federal Communications Commission regarding CPNI.
2. I hereby certify that, to the best of my knowledge, information and belief, BVU's operating procedures are adequate to ensure compliance with its CPNI obligations pursuant to Section 222 of the Communications Act of 1934, as amended, and the Commission's rules found at 47 CFR Subpart U.
3. Attached to this certification as Exhibit A is an accompanying statement explaining how the company's procedures ensure that the company is in compliance with the requirements set forth in section 64.2001 *et seq.* of the Commission's rules.



Brian C. Bolling, Vice President of Customer Service

February 19, 2010

Date

2009 CPNI Questionnaire For BVU

I. Use of CPNI for Marketing

- 1) Do you use CPNI to market any telecommunications or non-telecommunications services, either through your own sales force or through agents or other third parties?

Yes No

If response to Question 1 is NO, skip to question 8.

- 2) Do you use CPNI ONLY for one or more of the following purposes (See Section II of CPNI Summary):

- a) to market service offerings that are within the same category of service that you already provide to the customer (i.e., "total service approach"—see Section IIA of CPNI Summary)?
- b) to provide your customer with customer premises equipment, call answering, voice mail or messaging, voice storage or retrieval, fax store and forward, and protocol conversion?
- c) to provide inside wire installation, maintenance and repair services?
- d) for local carriers, to market features such as speed dialing, computer provided Directory Assistance, call tracing, call blocking, call return, repeat dialing, call tracking, call waiting, caller ID, call forwarding and certain centrex features?
- e) to protect your Company's rights or property?
- f) to protect your customers and other carriers from fraudulent, abusive or unlawful use or subscription of service?
- g) For CMRS providers only:
 - i) in conjunction with research on the health effects or CMRS.
 - ii) for the provision of CPE and information services.

Yes No

If the response to Question 2 is YES, no customer approval or notification is required -- skip to Question 5.

3) If you use CPNI for purposes other than those listed in Question 2, customer approval is required—please respond to the following questions:

- a) Explain your procedures for notifying customers of their right to restrict use of, disclosure, and access to their CPNI, prior to asking for approval to use CPNI. (See Section V.B. of CPNI Summary for notification requirements.)

If you use opt-out approval, do you provide notice to customers every two years?

Yes No

- b) Describe the procedures that you use for obtaining customer approval, establishing proof that approval was obtained, and maintaining records of customer approval. For instance, do you rely on opt-in approval (where the customer affirmatively agrees to the use of their CPNI), or Opt-Out approval (where the customer is required to notify you if they DO NOT want you to use their CPNI); do you rely on oral, written, and/or electronic methods of approval. (See Section V. of CPNI Summary)

4) If you use CPNI in a manner requiring customer approval, do you have a system that indicates the status of the customer's CPNI approval (e.g., a flag in the customer service record)? (See Section VI.A of CPNI summary)

Yes No

- 5) Do you train your personnel as to when they are and are not authorized to use CPNI and have a disciplinary process in place? (See Section VI. E of CPNI summary)

Yes No

Briefly describe.

BVU has a CPNI manual that covers disciplinary action and as part of the CPNI employees sign a document that acknowledges potential disciplinary action. For example an excerpt states, " Violation by Company employees and agents of such CPNI requirements will lead to prompt disciplinary action (up to and including remedial training, reprimands, unfavorable performance reviews, probation, and termination), depending upon the circumstances of the violation (including the severity of the violation, whether the violation was a first time or repeat violation, whether appropriate guidance was sought or received from the CPNI Compliance Officer(s), and the extent to which the violation was or was not deliberate or malicious).

- 6) Do you maintain a record of your company's and any affiliate's sales and marketing campaigns that use CPNI? (See Section VI.C of CPNI summary)

Yes No

- 7) Do you have a supervisory review process for compliance with CPNI rules for outbound marketing situations to ensure that sales personnel obtain supervisory approval of any proposed outbound marketing request for customer CPNI approval? (See Section VI.D and E of CPNI summary)

Yes No

Briefly describe the process and recordkeeping.

All outbound marketing situations must be approved by the Compliance Officer and after approval the effort is documented. The Compliance Officer will maintain a record of each outbound marketing activity or campaign, including:

- a. a description of the campaign;
 - b. the specific CPNI that was used in the campaign;
 - c. the date and purpose of the campaign;
 - d. the name and relationship of any third party to which CPNI was disclosed or provided, or which was allowed to access CPNI; and
 - e. what products and services were offered as part of the campaign.
-

- 8) Even if you do not use CPNI for marketing purposes, do you have processes in place to safeguard your customers' CPNI from (a) improper use or disclosure by your employees; and (b) attempts by third parties to gain unauthorized access to CPNI.

Yes No

Briefly describe the procedures you use.

Our CPNI manual covers the processes and they are included in our training. We have procedures that cover inbound calls from customer, outbound calls to customers, customer's request for CPNI whether in person or by phone, request by law enforcement, and protection and safeguarding of records.

- 9) Do you maintain a record of all instances where CPNI was disclosed or provided to third parties, or where third parties obtained access to CPNI? (See Section VI.G of CPNI Summary).

Yes No

II. Telephone Access to Call Detail – New FCC Rules

- 10) Do you provide call detail information (a subset of CPNI -- see Section I of CPNI summary for definition) over the telephone?

Yes No

If the response to Question 10 is NO -- skip to Question 11.

If the response to Question 10 is YES, please respond to the following questions:

- (a) Do you have procedures for establishing customer password, and authenticating a customer's identity before issuing a password without using readily available biographical information or account information? (See Section VII.A and C of CPNI Summary)

Yes No

Briefly explain your procedures.

Passwords can be designed in a manner that is privately significant and memorable to the customer (e.g., "pirates1971," "1836alamo," "\$beatles4"). However, passwords may NOT be based upon readily obtainable biographical information (e.g., the customer's name, mother's maiden name, social security number or date of birth) or account information (e.g., the customer's telephone number, address, account number, or amount of last bill).

- (b) Do you have a back-up authentication method for lost or forgotten passwords that does not prompt the customer for readily available biographical information or account information? (See Section VII.C of CPNI Summary)

Yes No

Briefly explain your method.

b. The Company will establish a password (and a back-up customer authentication method if the customer loses or forgets his or her password) for each new customer at the time that the customer initiates service.

c. The Company will establish a new or replacement password (and a back-up customer authentication method if the customer loses or forgets his or her password) for existing customers desiring a password pursuant to the following procedure. The Company may periodically announce on its website, in its newsletter and/or in its billing materials that customers must have a password for security and privacy purposes in order to call the Company and obtain their call detail information over the telephone. The

TMI Confidential.

For use by Clients of Technologies Management, Inc. only.

Company announcements will inform customers that they may obtain an initial or replacement password: (i) if they come in person to the Company's business office, produce a driver's license, passport or other government-issued identification verifying their identity, and correctly answer certain questions regarding their service and address; or (ii) if they call a specified Company telephone number from their "telephone number of record" (see definition above) and then wait at that number until a Company employee calls them back and obtains correct answers to certain questions regarding their service and address; or (iii) if they ask the Company to send a randomly-generated Personal Identification Number ("PIN") to their "telephone number of record" (see definition above) by voice, voicemail or text message or mail it to their "address of record" (see definition above), and then call the Company back and provide the correct PIN.

d. The Company's "back-up customer authentication method" will consist of a "shared secret" combination of two pre-selected questions by the Company and two pre-selected answers by the customer regarding two non-public aspects of the customer's life that would not be known by a pretexter, hacker or other unauthorized entity. For example, such "shared secret" questions and answers might relate to the customer's favorite Holiday, color, song, book, movie, food, or sports team, or in what city were you born (unless such characteristic are a matter of public record or known by a significant number of people). If the customer claims to have lost or forgotten his or her password, but can correctly provide the pre-selected answers to the two pre-selected "shared secret" questions, the requested call detail information can be given to the customer over the telephone during the customer-initiated call.

- (c) If a customer cannot provide the correct password or response to any back-up authentication methods, do you require them to establish a new password? (See Section VII.C of CPNI Summary)

Yes No

- (d) Do you have in place a process that ensures that call detail is not disclosed unless the customer either (i) provides a valid password or (ii) provides the call detail information that is the subject of the inquiry without a customer service representative's assistance? (See Section VII.B of CPNI Summary)

Yes No

- (e) If the customer does not provide a password or fall into the exception in (d)(ii) above, or if the customer seeks additional call detail information, do you only provide call detail by sending it to the customer's address of record or by calling the customer at the telephone number of record? (See Section VII.B of CPNI Summary)

Yes No

III. Online Access to CPNI – New FCC Rules

11) Do you provide online access to CPNI?

Yes No

If the response to Question 11 is NO – skip to Question 12.

If the response to Question 11 is YES, please respond to the following questions:

(a) Do you have procedures for establishing customer password for online access, and authenticating a customer's identity before issuing a password without using readily available biographical information or account information? (See Section VII.D of CPNI Summary)

Yes No

Briefly explain your procedures.

Customers may have access to their billing via internet access to our secure server. Customer must establish a User ID and Password by entering a 5 digit secret number in conjunction with their account number.

If your company is a wireline or wireless provider with fewer than 1500 employees or a interconnected VOIP provider with less than \$6 million in annual revenue you can delay implementation of the online authentication and password requirements until June 8, 2008. Please indicate below if this exemption applies and go to Question 12. Otherwise, respond to the following questions:

(b) Do you have a back-up authentication method for lost or forgotten passwords that does not prompt the customer for readily available biographical information or account information? Briefly explain your procedures. (See Section VII.C of CPNI Summary)

Yes No

- (c) If a customer cannot provide the correct password or response to any back-up authentication methods, do you require them to establish a new password? (See Section VII.C of CPNI Summary)

Yes No

- (d) Do you require a password before allowing online access? (See Section VII.C of CPNI Summary)

Yes No

IV. In-Store (Retail Location) Access to CPNI – New FCC Rules

- 12) Do you allow in-store access to CPNI?

Yes No

If the response to Question 12 is NO -- skip to Question 13.

If the Response to Question 12 is YES, answer the following question:

- (a) Do you only disclose CPNI if the customer has presented a valid photo ID matching his/her account information? (See Section VII.E of CPNI Summary)

Yes No

They can answer the password word in person too or respond to challenge questions.

V. Notification of Account Changes – New FCC Rules

- 13) Do you notify customers of the following types of account changes without revealing the changed information or sending the notification to the new account information: (i) password changes; (ii) change to a response to a back-up means of authentication; (iii) change to online account; (iv) change or creation of an address of record (other than at service initiation)?

Yes No

Briefly explain the method of notification used (e.g., carrier originated voice mail, text message to phone number of record, or mail to the address of record). (See Section VII.F of CPNI Summary)

The notice may be provided by: (i) a Company call or voicemail to the customer's telephone number of record; (ii) a Company text message to the customer's telephone number of record; or (iii) a written notice mailed to the customer's address of record (to the customer's prior address of record if the change includes a change in the customer's address of record).

VI. Notification of CPNI Breaches – New FCC Rules

14. (a) Do you have in place procedures to notify law enforcement (the United States Secret Service and the FBI) of a breach of a customer's CPNI within 7 business days? (See Section VIII.A of CPNI Summary)
- Yes No
- (b) Do you have in place procedures to notify customers of the breach, but only 7 business days after notification to law enforcement? (See Section VIII.B of CPNI Summary)
- Yes No
- (c) Do you maintain records of: (i) any breaches discovered; (ii) notifications made to the USSS and FBI; and (iii) notifications made to customers?
- Yes No
- (d) Do your records include the dates of discovery and notification, a detailed description of the CPNI that was breached and the circumstances of the breach? (See Section VIII.C of CPNI Summary)
- Yes No

VII. Actions Against Data Brokers – New FCC Rules

- 15) Have you taken any actions against data brokers in the last year?

Yes No

If yes, explain the actions taken.

VIII. Customers Complaints about CPNI – New FCC Rules

- 16) Did you receive any complaints about unauthorized release or disclosure of CPNI from December 8, 2007 (effective date of new rules) through December 31, 2007?

Yes No

If the response to Question 16 is YES, please respond to the following questions:

Provide the total number of complaints received broken down by the following categories: (a) instances of improper access by employees; (b) instances of improper disclosure to individuals not authorized to receive the information; (c) instances of improper access to online information by individuals not authorized to view the information.

IX. Pretexters Processes

- 17) Have you developed any information with respect to the processes that pretexters are using to attempt to access CPNI?

Yes No

If so, provide the information.

We have stated the following in our CPNI manual: In some unfortunate instances, pretexters have obtained CPNI from telephone company representatives who have cooperated for friendship, financial or other reasons. The Company will take any and all disciplinary, termination and/or remedial actions permitted by applicable federal and state employment law against any Company representative that is reasonably suspected to have cooperated knowingly and intentionally with a pretexter.

Pretexters may use a variety of tactics to try to fool telephone company representatives in order to get unauthorized and unlawful access to CPNI. Some of these tactics involve mock anger and bullying; others entail pleading and playing upon normal human emotions.

Statement of CPNI Procedures and Compliance

Use of CPNI

Bristol Virginia Utilities (“BVU”) does not use or permit access to CPNI to market any services outside of the total service approach as specified in 47 CFR §64.2005. If BVU elects to use CPNI in a manner that does require customer approval, it will follow the applicable rules set forth in 47 CFR Subpart U, including the institution of operational procedures to ensure that notification is provided and customer approval is obtained before CPNI is used or disclosed.

PROTECTION OF CPNI

BVU has put into place processes to safeguard its customers’ CPNI/call detail information from improper use or disclosure by employees; and to discover and protect against attempts by third parties to gain unauthorized access to customer CPNI. BVU has a CPNI manual that covers disciplinary action and as part of the CPNI procedures employees sign a document that acknowledges potential disciplinary action. For example an excerpt states: *Violation by Company employees and agents of such CPNI requirements will lead to prompt disciplinary action (up to and including remedial training, reprimands, unfavorable performance reviews, probation, and termination), depending upon the circumstances of the violation (including the severity of the violation, whether the violation was a first time or repeat violation, whether appropriate guidance was sought or received from the CPNI Compliance Officer(s), and the extent to which the violation was or was not deliberate or malicious).*

IF COMPANY USES CPNI:

BVU ensures that all access to CPNI be approved by a supervisor with knowledge of the FCC’s CPNI requirements. BVU has instituted training procedures and a corresponding disciplinary process to ensure that its personnel understand and comply with restrictions regarding the use and disclosure of, and access to, CPNI. All outbound marketing situations must be approved by the Compliance Officer and after approval the effort is documented. The Compliance Officer will maintain a record of each out-bound marketing activity or campaign, including:

- a. a description of the campaign;
- b. the specific CPNI that was used in the campaign;
- c. the date and purpose of the campaign;
- d. the name and relationship of any third party to which CPNI was disclosed or provided, or which was allowed to access CPNI; and
- e. what products and services were offered as part of the campaign.

DISCLOSURE OF CALL DETAIL OVER PHONE

BVU has instituted authentication procedures to safeguard the disclosure of call detail over the telephone. BVU's authentication procedures do not require the use of readily available biographical information or account information as defined by the FCC. BVU procedures allow that passwords can be designed in a manner that is privately significant and memorable to the customer (e.g., "pirates1971," "1836alamo," "\$beatles4"). However, passwords may NOT be based upon readily obtainable biographical information (e.g., the customer's name, mother's maiden name, social security number or date of birth) or account information (e.g., the customer's telephone number, address, account number, or amount of last bill). All customers are required to establish a password without the use of readily available biographical information or account information if they want to receive call detail over the telephone. If the appropriate password is not provided, BVU does not disclose call detail over the telephone.

BVU has established back-up authentication procedures for lost or stolen passwords that do not prompt the customer for readily available biographical information or account information. Company's back-up authentication procedure operates as follows (excerpt from the Company's CPNI manual):

b. The Company will establish a password (and a back-up customer authentication method if the customer loses or forgets his or her password) for each new customer at the time that the customer initiates service.

c. The Company will establish a new or replacement password (and a back-up customer authentication method if the customer loses or forgets his or her password) for existing customers desiring a password pursuant to the following procedure. The Company may periodically announce on its website, in its newsletter and/or in its billing materials that customers must have a password for security and privacy purposes in order to call the Company and obtain their call detail information over the telephone. The Company announcements will inform customers that they may obtain an initial or replacement password: (i) if they come in person to the Company's business office, produce a driver's license, passport or other government-issued identification verifying their identity, and correctly answer certain questions regarding their service and address; or (ii) if they call a specified Company telephone number from their "telephone number of record" (see definition above) and then wait at that number until a Company employee calls them back and obtains correct answers to certain questions regarding their service and address; or (iii) if they ask the Company to send a randomly-generated Personal Identification Number ("PIN") to their "telephone number of record" (see definition above) by voice, voicemail or text message or mail it to their "address of record" (see definition above), and then call the Company back and provide the correct PIN.

d. The Company's "back-up customer authentication method" will consist of a "shared secret" combination of two pre-selected questions by the Company and two pre-selected answers by the customer regarding two non-public

aspects of the customer's life that would not be known by a pretexter, hacker or other unauthorized entity. For example, such "shared secret" questions and answers might relate to the customer's favorite Holiday, color, song, book, movie, food, or sports team, or in what city were you born (unless such characteristic are a matter of public record or known by a significant number of people). If the customer claims to have lost or forgotten his or her password, but can correctly provide the pre-selected answers to the two pre-selected "shared secret" questions, the requested call detail information can be given to the customer over the telephone during the customer-initiated call.

Company has put into place procedures to notify 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 without revealing the changed information or sending the notification to the new account information. The notice may be provided by: (i) a Company call or voicemail to the customer's telephone number of record; (ii) a Company text message to the customer's telephone number of record; or (iii) a written notice mailed to the customer's address of record (to the customer's prior address of record if the change includes a change in the customer's address of record).

DISCLOSURE OF CPNI ONLINE

BVU has instituted authentication procedures to safeguard the disclosure of CPNI on-line. BVU's authentication procedures do not require the use of readily available biographical information or account information as defined by the FCC. Customers may have access to their billing via internet access to our secure server. Customer must establish a User ID and Password by entering a 5 digit secret number in conjunction with their account number. Unless the appropriate password is provided, BVU does not allow on-line access to CPNI.

BVU has established back-up authentication procedures for lost or stolen passwords that do not prompt the customer for readily available biographical information or account information. See above excerpt from BVU's CPNI manual.

Company has put into place procedures to notify 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 without revealing the changed information or sending the notification to the new account information. The notice may be provided by: (i) a Company call or voicemail to the customer's telephone number of record; (ii) a Company text message to the customer's telephone number of record; or (iii) a written notice mailed to the customer's address of record (to the customer's prior address of record if the change includes a change in the customer's address of record).

DISCLOSURE OF CPNI AT RETAIL LOCATIONS

Company discloses CPNI at its retail locations only if the customer has presented a valid photo ID matching his/her account information.

NOTIFICATION TO LAW ENFORCEMENT

Company has in place procedures to notify law enforcement in the event of a breach of customers' CPNI and to ensure that customers are not notified of the breach before the time period set forth in the FCC's rules, or, if applicable, when so authorized by law enforcement.

BVU maintains records of all breaches discovered and notifications made to the USSS and the FBI, and to customers.

ACTIONS AGAINST DATA BROKERS

Company has not taken any actions against data brokers in the last year.

CUSTOMER COMPLAINTS ABOUT CPNI BREACHES

Company did not receive any customer complaints about the unauthorized release of CPNI or the unauthorized disclosure of CPNI in calendar year 2008.

INFORMATION ABOUT PRETEXTERS

Company has developed the following information with respect to the processes pretexters are using to attempt to access CPNI and is taking the following steps to protect CPNI. BVU has stated the following in its CPNI manual:

In some unfortunate instances, pretexters have obtained CPNI from telephone company representatives who have cooperated for friendship, financial or other reasons. The Company will take any and all disciplinary, termination and/or remedial actions permitted by applicable federal and state employment law against any Company representative that is reasonably suspected to have cooperated knowingly and intentionally with a pretexter.

Pretexters may use a variety of tactics to try to fool telephone company representatives in order to get unauthorized and unlawful access to CPNI. Some of these tactics involve mock anger and bullying; others entail pleading and playing upon normal human emotions.