



## Davis Wright Tremaine LLP

ANCHORAGE BELLEVUE LOS ANGELES NEW YORK PORTLAND SAN FRANCISCO SEATTLE SHANGHAI WASHINGTON, D.C.

PAUL HUDSON  
DIRECT (202) 973-4275  
paulhudson@dwt.com

SUITE 200  
1919 PENNSYLVANIA AVE NW  
WASHINGTON, DC 20006

TEL (202) 973-4200  
FAX (202) 973-4499  
www.dwt.com

February 27, 2009

### VIA ELECTRONIC FILING

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

**Re: EB Docket 06-36, Annual 47 C.F.R. § 64.2009(e) CPNI Certification**

Annual § 64.2009(e) CPNI Certification for 2008

Date filed: February 27, 2009

Name of companies covered by this certification:

**Bresnan Communications, LLC**

**Bresnan Broadband of Montana, LLC**

**Bresnan Broadband of Wyoming, LLC**

**Bresnan Broadband of Colorado, LLC**

**Bresnan Broadband of Utah, LLC**

Form 499 Filer ID: **824408** (Bresnan Communications, LLC)

Name of signatory: **Jerold C. Lambert**

Title of signatory: **Vice President and Associate General Counsel**

Dear Ms. Dortch:

Pursuant to Section 64.2009(e) of the Commission's Rules, 47 C.F.R. § 64.2009(e), enclosed for filing in the above-referenced docket is the executed annual CPNI Compliance Certificate of Bresnan Communications, LLC and its operating subsidiaries Bresnan Broadband of Montana, LLC; Bresnan Broadband of Wyoming, LLC; Bresnan Broadband of Colorado, LLC; and Bresnan Broadband of Utah, LLC (together, "Company").

Attached to the certificate is a summary of Company's CPNI policies and procedures. Because some of the details included in that document could provide a roadmap for unauthorized

Ms. Marlene H. Dortch  
Secretary  
Federal Communications Commission  
February 27, 2009  
Page 2

persons to attempt to obtain CPNI, Company is filing only a redacted version with the Commission's electronic filing system. *See Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, CC Docket No. 96-115, Report and Order and Further Notice of Proposed Rulemaking, FCC 07-22, n.167 (rel. April 2, 2007) ("We recognize carrier concerns about providing a roadmap for pretexters with this annual filing, and thus we will allow carriers to submit their certifications confidentially with the Commission."). The redacted language was previously provided to the Enforcement Bureau in Company's prior-year filing in this docket, and has not changed.

Respectfully submitted,

A handwritten signature in black ink, appearing to read "PBH", written in a cursive style.

Paul B. Hudson  
Counsel for Bresnan Communications, LLC

Enclosures

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

**EB Docket 06-36**

Annual 64.2009(e) CPNI Certification for 2008

Date filed: February 27, 2009

Name of companies covered by this certification:

**Bresnan Communications, LLC  
Bresnan Broadband of Montana, LLC  
Bresnan Broadband of Wyoming, LLC  
Bresnan Broadband of Colorado, LLC  
Bresnan Broadband of Utah, LLC**

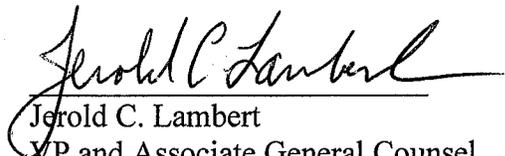
Form 499 Filer ID: **824408** (Bresnan Communications, LLC)

Name of signatory: **Jerold C. Lambert**

Title of signatory: **Vice President and Associate General Counsel**

I, Jerold C. Lambert, certify that I am an officer of each of the companies named above (together, "Company") and, acting as an agent of the Company, that I have personal knowledge that the Company has established operating procedures, summarized in the attached statement, that are adequate to ensure compliance with the Commission's rules governing use and disclosure of confidential proprietary network information ("CPNI"), as governed by Section 222 of the Communications Act of 1934, as amended by the Telecommunications Act of 1996, and as set forth in Part 64, Subpart U of the of the Commission's rules, 47 C.F.R. §§ 64.2001 *et seq.*

The Company has not received any customer complaints in the past calendar year concerning unauthorized access to or release of CPNI. Company does not have any material information with respect to the processes pretexters are using to attempt to access CPNI that is not already a part of the record in the Commission's CC Docket No. 96-115. Company has therefore not taken any actions in the past year against data brokers, including proceedings instituted or petitions filed by the company at either state commissions, the court system or at the Commission. The Company has established procedures to report any breaches to the FBI and United States Secret Service, and it has emphasized in its employee training of the need for vigilance in identifying and reporting unusual activity in order to enable the Company to continue to take reasonable measures to discover and protect against pretexting and other unauthorized access to CPNI.

  
Jerold C. Lambert

VP and Associate General Counsel  
Bresnan Communications, LLC  
Bresnan Broadband of Montana, LLC  
Bresnan Broadband of Wyoming, LLC  
Bresnan Broadband of Colorado, LLC  
Bresnan Broadband of Utah, LLC  
Executed February \_\_, 2009

## **CPNI Compliance Policies of Bresnan Communications**

*Effective December 8, 2007*

Bresnan Communications, LLC; Bresnan Digital Services, LLC; Bresnan Broadband of Montana, LLC; Bresnan Broadband of Wyoming, LLC; Bresnan Broadband of Colorado, LLC; and Bresnan Broadband of Utah, LLC (collectively, “Bresnan”) have implemented the following policies and procedures as of December 8, 2007 that are designed to protect the confidentiality of Customer Proprietary Network Information (“CPNI”) and to assure compliance with the rules of the Federal Communications Commission (“FCC”) set forth in 47 C.F.R. Part 64, Subpart U, Section 2001 *et seq.*, including the FCC’s new rules adopted in *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers’ Use of Customer Proprietary Network Information and Other Customer Information*, CC Docket No. 96-115, Report and Order and Further Notice of Proposed Rulemaking, FCC 07-22 (rel. April 2, 2007).

CPNI is (A) information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and (B) information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier.

Bresnan trains employees on the limitations of use or disclosure of CPNI as governed by federal law and Bresnan policy. Bresnan’s policy, administered by its CPNI Compliance Officer Jerry Lambert, Bresnan’s Vice President and Associate General Counsel, establishes the procedures and safeguards regarding Bresnan’s use and disclosure of CPNI set forth below.

[REDACTED]

### **I. USE, DISCLOSURE OF, AND ACCESS TO CPNI**

Bresnan will use, disclose, or permit access to CPNI only in its provision of the communications service from which such information is derived; for services necessary to, or used in, the provision of such communications service, including the publishing of directories; to initiate, render, bill and collect for communications services; to protect the rights or property of Bresnan, or to protect users or other carriers or service providers from fraudulent, abusive or unlawful use of, or subscription to, such services; to provide inside wiring installation, maintenance, or repair services; as required by law; or as expressly authorized by the customer.

Bresnan does not use CPNI to market services. Bresnan has established a supervisory review process regarding its compliance with the FCC’s CPNI rules for marketing situations and maintains records of carrier compliance for a minimum period of one year. In the event that any employee or agent wishes to use CPNI for marketing, such proposed use is subject to a supervisory review process that shall involve a supervisor designated by the senior employee responsible for marketing or the CPNI Compliance Officer. If such use is approved, Bresnan shall modify these policies and conduct additional training as needed to assure compliance with the FCC’s rules.

## **PUBLIC VERSION**

Bresnan does not use, disclose or permit access to CPNI to identify or track customers that call competing service providers.

When Bresnan receives or obtains proprietary information from another carrier for purposes of providing a telecommunications service, it shall use such information only for such purpose, and shall not use such information for its own marketing efforts.

### **II. SAFEGUARDS AGAINST DISCLOSURE OF CPNI TO UNAUTHORIZED PARTIES**

Above and beyond the specific FCC requirements, Bresnan will take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI. If any employee becomes aware of new methods that are being used or could be used by third parties to attempt to obtain unauthorized access to CPNI, or of possible changes to Bresnan's existing policies that would strengthen protection of CPNI, they should report such information immediately to Bresnan's CPNI Compliance Officer so that Bresnan may evaluate whether existing policies should be supplemented or changed.

#### **A. Inbound Calls to Bresnan Requesting CPNI**

CSRs may not disclose any CPNI to an inbound caller until the caller's identity has been authenticated. For CPNI not including Call Detail Information (CDI), CSRs authenticate callers by requesting [REDACTED].

Bresnan CSRs do not reveal any Call Detail Information (CDI) to inbound callers. The CSRs that answer inbound telephone calls do not have access to CDI. CDI includes any information that pertains to the transmission of specific telephone calls, including, for outbound calls, the number called, and the time, location, or duration of any call and, for inbound calls, the number from which the call was placed, and the time, location, or duration of any call.

[REDACTED] Bresnan's ordinary policy is to provide the requested CDI by sending the information by mail to a mailing address of record for the account, but only if such address has been on file with Bresnan for at least 30 days. [REDACTED]

#### **B. Online Accounts**

Bresnan customers may obtain certain telephone account information from certain online sources accessed from the Bresnan website. To access these on-line accounts, the customer must enter a login ID that they create and a password established in accordance with the criteria set forth below.

The first online portal, Bresnan's billing portal, provides customers with online access to their consolidated cable, broadband and telephone bills, and permits them to view and pay their bill. The second portal, the Call Detail portal, permits customers to view CDI from calls within the past 30 days and some other CPNI, such as the amount of their telephone bill.

[REDACTED]

## **PUBLIC VERSION**

### **C. In-Person Disclosure of CPNI at Bresnan Offices**

Bresnan may disclose CPNI to a customer visiting a Bresnan office if they present a valid photo ID matching the customer's account information. A "valid photo ID" is a government-issued means of personal identification with a photograph such as a driver's license, passport, or comparable ID that is not expired.

### **D. Notice of Account Changes**

When an online account is created or when a password or PIN is changed, Bresnan will mail a notification to customer's address of record notifying them of the change. When an address of record is created or changed, Bresnan will send a notice to customer's preexisting address of record notifying them of the change. These notifications are not required when the customer initiates service. Each of the notices provided under this paragraph will not reveal the changed information and will direct the customer to notify Bresnan if they did not authorize the change.

### **E. Business Customer Exemption**

Pursuant to 47 C.F.R. § 64.2010(g), the authentication requirements for disclosure of CPNI do not apply to disclosure of business customer information where the business customer has a dedicated account representative and a contract between Bresnan and that business customer that specifically addresses the protection of CPNI.

### **F. Audit Trail**

[REDACTED]

### **G. Data Retention**

[REDACTED]

## **III. REPORTING CPNI BREACHES TO LAW ENFORCEMENT**

Any Bresnan employee that becomes aware of any breaches, suspected breaches or attempted breaches must report such information immediately to the Bresnan CPNI Compliance Officer. Such information must not be reported or disclosed by any employee to any non-employee, including the potentially affected customer, except in express conformance with the procedures described below. Any employee that fails to report such information will be subject to disciplinary action that may include termination.

Bresnan's CPNI Compliance Officer is Jerry Lambert, [REDACTED].

It is Bresnan's policy that employees should not be discouraged from reporting information about breaches that may have been caused in part by their own actions or omissions. Once a breach has occurred, the most important objective is to attempt to limit the damage to customers, to make any adjustments as needed to prevent a recurrence of the breach, and to alert law enforcement promptly. Therefore, although employees who violate Bresnan's CPNI policies are

## **PUBLIC VERSION**

subject to discipline, the sanctions may be substantially reduced where employees promptly self-report violations if appropriate.

### **A. Identifying a “Breach”**

A “breach” has occurred when a person, without authorization or exceeding authorization, has intentionally gained access to, used, or disclosed CPNI. If an employee has information about an incident and is not certain that the incident would not constitute a breach under this definition, the incident must be reported to the CPNI Compliance Officer.

If a Bresnan employee determines that an unauthorized person is attempting to gain access to CPNI but does not succeed at doing so, no breach has occurred. However, the incident must be reported to Bresnan’s CPNI Compliance Officer who will determine whether to report the incident to law enforcement and/or take other appropriate action. Bresnan’s CPNI Compliance Officer will also determine whether it is appropriate to update Bresnan’s CPNI policies or training materials in light of any new information.

### **B. Notification Procedures**

As soon as practicable, and in no event later than 7 business days upon learning of a breach, the Bresnan CPNI Compliance Officer shall electronically notify the United States Secret Service (USSS) and the Federal Bureau of Investigation (FBI) by accessing the following link: <https://www.cpnireporting.gov>. Company’s FRN number and password may be required to submit a report. If this link is not responsive, they should contact counsel or the FCC’s Enforcement Bureau (202-418-7450 or <http://www.fcc.gov/eb/cpni>) for instructions.

Bresnan will not notify customers or disclose a breach to the public until 7 full business days have passed after notification to the USSS and the FBI, except as provided below (a full business day does not count a business day on which the notice was provided). Federal law requires compliance with this requirement even if state law requires disclosure. If Bresnan receives no response from law enforcement after the 7<sup>th</sup> full business day, it must promptly proceed to inform the customers whose CPNI was disclosed of the breach.

Bresnan will delay notification to customers or the public upon request of the FBI or USSS.

If the Bresnan CPNI Compliance Officer believes there is a need to disclose a breach sooner, he or she should so indicate in the notification to law enforcement. However, such notification does not itself permit notice to customers; Bresnan still may not notify customers sooner unless given clearance to do so from *both* the USSS and the FBI.

## **IV. RECORD RETENTION**

The Bresnan CPNI Compliance Officer is responsible for assuring that we maintain for at least two years a record, electronically or in some other manner, of any breaches discovered, notifications made to the USSS and the FBI pursuant to these procedures, and notifications of breaches made to customers. The record must include, if available, dates of discovery and

## **PUBLIC VERSION**

notification, a detailed description of the CPNI that was the subject of the breach, and the circumstances of the breach.

Bresnan maintains a record, for a period of at least one year, of: those limited circumstances in which CPNI is disclosed or provided to third parties or where third parties were allowed access to CPNI. Because Bresnan does not use CPNI for marketing or for any other purpose for which customer approval is required, it does not have any records to keep regarding supervisory review of marketing; or of sales and marketing campaigns that use CPNI; or of records associated with customers' "opt-out" approval or non-approval to use CPNI, or notification to customers prior to any solicitation for customer approval to use or disclose CPNI.

Bresnan will maintain a record for at least two years of any customer complaints related to its handling of CPNI, and records of Bresnan's handling of such complaints. The CPNI Compliance Officer will assure that all complaints are reviewed and that Bresnan considers any necessary changes to its policies or practices to address the concerns raised by such complaints.

Bresnan will have an authorized corporate officer, as an agent of the company, sign a compliance certificate on an annual basis stating that the officer has personal knowledge that Bresnan has established operating procedures that are adequate to ensure its compliance with FCC's CPNI rules. The certificate for each year will be filed with the FCC Enforcement Bureau in EB Docket No. 06-36 by March 1 of the subsequent year, and will be accompanied by a summary or copy of this policy that explains how Bresnan's operating procedures ensure that it is in compliance with the FCC's CPNI rules. In addition, the filing must include 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 CPNI. Confidential portions of these submissions shall be redacted from the public version of the filing and provided only to the FCC.

## **V. TRAINING**

[REDACTED] All employees with such access receive a copy of Bresnan's CPNI policies and are informed that (i) any use or disclosure of CPNI or other act or omission not in compliance with such policies will result in disciplinary action, including the termination of employment where appropriate, and (ii) employees who knowingly facilitate the unauthorized disclosure of a customer's confidential information may be subject to criminal penalties. In addition, Bresnan conducts mandatory CPNI training for all CSRs, personnel at retail offices that may receive requests for CPNI, technical support personnel who field calls from customers, provisioning personnel who have access to and research customer inquiries regarding CDI, and marketing personnel. Initial training was completed prior to December 8, 2007. [REDACTED]