Green Hills Telephone Corporation

7926 NE State Route M, P.O. Box 227
Breckenridge, MO 64625
PHONE: (660) 644-5411 FAX (660) 644-5464
www.greenhills.net

Serving the area since 1952

EB-06-TC-060
EB Docket No. 06-36

CERTIFICATION OF CPNI FILING MARCH 1, 2010

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

Dear Secretary Dortch:

In accordance with the Public Notice issued by the Enforcement Bureau on January 30, 2006, please find attached our company's annual compliance certificate for the most recent period as required by section 64.2009(e) of the Commission's Rules together with a statement of our company's operating procedures established to ensure compliance with the Commission's Rules and Regulations regarding Customer Proprietary Network Information.

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

Sincerely,

Renee' Reeter
Controller

Cc: BCPI via email fcc@bcpiweb.com

7926 NE State Route M, P.O. Box 227
Breckenridge, MO 64625
PHONE: (660) 644-5411 FAX (660) 644-5464
www.greenhills.net

Green Hills Telephone Corporation

Serving the area since 1952

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

EB Docket 06-36

Annual 64.2009(e) CPNI Certification for 2009

Date filed: 1/19/2010

Name of company(s) covered by this certification: Green Hills Telephone Corporation

Form 499 Filer ID: 808936

Name of signatory: Renee' Reeter

Title of signatory: Controller

I, Renee' Reeter, certify that I am authorized by 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 set forth in section 64.2001 *et seq.* of the Commission's rules.

The company has not taken any actions (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. Companies must report on any information that they have with respect to the processes pretexters are using to attempt to access CPNI , and what steps companies are taking to protect CPNI.

The company has not received any customer complaints in the past year concerning the unauthorized release of CPNI (number of customer complaints a company has received related to unauthorized access to CPNI, or unauthorized disclosure of CPNI, broken down by category or complaint, *e.g.*, instances of improper access by employees, instances of improper disclosure to individuals not authorized to receive the information, or instances of improper access to online information by individuals not authorized to view the information).

Signed _____

STATEMENT OF PROCEDURES ADOPTED BY Green Hills Telephone Corporation TO ENSURE COMPLIANCE WITH THE RULES AND REGULATIONS OF THE FEDERAL COMMUNCIATIONS COMMISSION REGARDING THE PROTECTION OF CUSTOMER PROPRIETARY NETWORK INFORMATION ("CPNI")

Our Company has elected to utilize CPNI for purpose other than those purposes that are permissible without customer approval in accordance with Section 64.2005 of the FCC's Rules and Regulations. We utilize this information in accordance with Sections 64.2007 and 64.2009 of the FCC's Rules and Regulations. We provide our customers notification of their rights with respect to their CPNI and have adopted the "opt out" approval method. We take necessary safeguards on the disclosure of CPNI in accordance with Section 64-2010 of the FCC's Rules and Regulations. In the event of security breaches, we will take steps as outline in Section 64-2011 of the FCC's Rules and Regulations. We have adopted the procedures set forth below to ensure our familiarity and compliance with the applicable rules for any purpose that requires customer approval.

CPNI Use (§64-2005)

(1) We recognize that we may use, disclose or permit access to CPNI to protect our rights and property, our Customers, and other carriers from fraudulent, abusive or unlawful use of, or subscription to, our services.
(2) We understand that we may use, disclose or permit access to CPNI to provide or market service offerings among the categories of service to which the Customer already subscribes. When we provide different categories of service, and a Customer subscribes to more than one service category, we understand that we may share the Customer's CPNI with the affiliate that provides service to the Customer; but if a Customer subscribes to only one service category, we may not share the customer's CPNI with an affiliate without the Customer's approval.
(3) We understand that we may use, disclose or permit access to CPNI derived from our provision of local exchange or interexchange service for the provision of CPE and call answering, voice mail or messaging, voice storage and retrieval services, fax store-and-forward, and protocol conversion, without Customer approval,
(4) In the absence of Customer approval, we do 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 that we understand that we may use, disclose or permit access to CPNI to: (a) provide inside wiring installation, maintenance and repair services; and (b) market, when we provide local service, services formerly known as

adjunct-to-basic services such as, but not limited to, speed dialing, computer-provided directory assistance, all monitoring, call tracing, call blocking, call return, repeat dialing, call tracking, call waiting, caller ID, call forwarding, and certain Centrex features.

(5) We do not use, disclose or permit access to CPNI to identify or track Customers that call competing service providers. For example, as a local exchange carrier, we do not use local service CPNI to track Customers that call local service competitors.

Required Procedures to Obtain Customer Approval to Use CPNI (§64-2007)

(1) When we seek to utilize, disclose or permit access to CPNI in an instance where Customer approval is required, we obtain approval through written or oral methods. When we rely on oral approval, we understand we bear the burden of demonstrating that such approval was given in compliance with the CPNI rules. We honor a Customer's approval or disapproval until the Customer revokes or limits such approval or disapproval. We will maintain all records of Customer approvals for at least one year.

(2) Subject to "opt-out" approval requirements, we understand that we may use a Customer's individually identifiable CPNI to market communications related services to that Customer, and that we may disclose that CPNI to our affiliates that provide communications-related services.

CPNI Notice Requirement Procedures (§64-2008)

(1) We individually notify and inform each Customer of his or her right to restrict the use or disclosure of, and access to, CPNI. When we seek to utilize, disclose or permit access to CPNI in an instance where Customer approval is required, we solicit approval using the "opt out" method, and we will maintain records of notification, whether oral or written, for at least one year.

(2) When we seek to utilize, disclose or permit access to CPNI in an instance where Customer approval is required, our notifications provide information sufficient to enable our Customers to make informed decisions as to whether to permit the use or disclosure of, or permit access to, their CPNI. Our notifications: (a) contain a statement that the Customer has a right, and we have a duty, under federal law, to protect the confidentiality of CPNI; (b) specify the types of information that constitute CPNI and the specific entities that will receive CPNI, describe the purposes for which the CPNI will be used, and inform the Customer of his or her right to disapprove those uses and deny or withdraw access to CPNI use at any time. With regard to the latter, we will indicate that any approval, or disapproval, will remain in effect until the Customer affirmatively revokes or limits such approval or denial.

(3) We utilize the "opt out" method so when we seek to utilize, disclose or permit access to CPNI in an instance where Customer approval is required, we advise the Customer of the precise steps the Customer must take in order to grant or deny access to CPNI, and we clearly state that a denial of approval will not affect the provision of any services to which the Customer subscribes. We understand that in any such notification we must also provide a brief statement, in clear and neutral language, that describes the consequences directly resulting from the lack of access to CPNI. In addition, we understand that we must state that the Customer's consent to use his or her CPNI may enhance our ability to offer products and services tailored to meet the Customer's needs and that we will disclose the Customer's CPNI to any person upon the affirmative written request of the Customer.

(4) When we seek to utilize, disclose or permit access to CPNI in an instance where Customer approval is required, our notifications are comprehensible and not misleading and, when written, are legible, sufficiently in large type, and placed in an area readily apparent to the Customer. And, if any portion of any such notification is in another language, all portions of the notification will be in that language.

(5) We do not include in any such notification any statement that attempts to encourage a Customer to freeze third-party access to CPNI.

(6) For "opt-out" approvals, we understand that our notifications must satisfy items (1) – (5) above. We do not use oral notifications except in the event that a need arises to obtain limited, one-time use of CPNI for inbound and outbound customer telephone contacts for the duration of the call, regardless of whether we use "opt-out" or "opt-in" approval based on the nature of the contact. When we use oral notice in this manner, we comply with items (1) – (5) above, except that, if none of the following situations are relevant to the limited use for which we seek CPNI, we will not: (a) advise Customers, if they have opted out previously, that no action is needed to maintain the "opt-out" election; (b) advise Customers that we may share CPNI with our named or unnamed affiliates or third parties if the limited CPNI usage does not result in use by, or disclosure to, an affiliate or third party; (c) disclose the means by which a Customer can deny or withdraw future access to CPNI, so long as we explain that the scope of the approval is limited to one-time use; and (d) disclose the precise steps a Customer must take to grant or deny access to CPNI, so long as we clearly communicate that the Customer can deny access to his or her CPNI for the call.

(7) In addition, for "opt-out" approvals, we understand that we must wait at least 30 days after giving Customers notice and an opportunity to opt-out before assuming Customer approval to use, disclose, or permit access to CPNI and notify Customers of the applicable waiting period for a response before approval is assumed. We utilize the opt-out mechanism and provide notices to customers every two years.

(8) We do not use but in the event we used electronic notifications, we recognize that the waiting period begins to run on the date the notification is sent and, for mail notifications, it begins to run on the third day following the date the notification was mailed. In the event we utilize e-mail to provide opt-out notices, in addition to other requirements, we will: (a) obtain express, verifiable, prior approval to sending notices by e-mail regarding a Customer's service in general or their CPNI in particular; (b) allow Customers to reply directly to e-mails in order to opt-out; (c) use another means of communicating the notice if the e-mail is returned as undeliverable before considering the Customer to have received notice; and (d) ensure that the subject line in the e-mail clearly and accurately identifies the subject matter of the e-mail.

(9) With the use of the "opt-out" approvals, we also make available to every customer a method to opt-out that is of no additional cost to the Customer and is available 24 hours a day, seven days a week. We satisfy this requirement through a combination of methods, but we allow Customers to opt-out at no cost and whenever they choose.

CPNI Safeguard Procedures for use of CPNI (§64-2009)

(1) As described in this section, we have implemented a system by which the status of a Customer's CPNI approval can be clearly established prior to the use of the CPNI.

(2) We have trained our personnel as to when they are, and are not, authorized to use CPNI, and we have an express disciplinary process in place.

(3) We will maintain a record of any instance of our own and our affiliates' sales and marketing campaigns that use Customers' CPNI. In the event that we utilize, disclose, or permit access to CPNI in accordance with a Customer's approval, we will maintain a record of all such instances where CPNI was disclosed or provided to third parties or where third parties were allowed access to CPNI. The records include 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. We will retain these records for at least one year.

(4) We have established a supervisory review process regarding compliance with the CPNI rules for outbound marketing situations and, when we seek to utilize, disclose or permit access to CPNI for outbound marketing situations, we maintain compliance records for at least one year. Specifically, our sales personnel are required to obtain supervisory approval of any proposed outbound marketing request for customer approval of the use of CPNI.

(5) A corporate officer who acts as an agent for the Company signs a compliance certificate on an annual basis stating that the officer has personal knowledge that the Company has established these operating

procedures adequate to ensure compliance with applicable CPNI rules. This Statement of procedures which sets forth our operating procedures and demonstrates compliance with the CPNI rules will be maintained together with the compliance certificate. [1]Annually, effective March 1, the Company will file a compliance certificate which is accompanied by a statement explaining how its operating procedures ensure that it is or is not in compliance with the rules of Section 64-2009 (e). In addition, Company will 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. This filing will be made annually with the Enforcement Bureau on or before March 1 in EB Docket No. 06-36, for data pertaining to the previous year.

(6) In the event that we seek to utilize, disclose or permit access to CPNI in an instance where Customer approval is required, and we utilized an opt-out mechanism, we will provide written notice within five business days to the FCC and the Missouri Public Service Commission (MOPSC) of any instance where the opt-out mechanisms do not work properly to such a degree that consumers' inability to opt-out is more than an anomaly. Any such notice will be provided in the form of a letter that will include our 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 relevant state commission(s) were notified and what action was taken, a copy of any notice provided to customers, and contact information. We will submit any such notice even if other methods by which consumers may opt-out are offered.

Safeguard Procedures on the disclosure of CPNI (§64-2010)

(1) We take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI. We properly authenticate a customer prior to disclosing CPNI based on a customer initiated telephone contact or an in-store visit. We do not currently have online account access; therefore it is not an issue. We have established a password on customer account to assist in that identification for customer initiated calls and do not ask for biographical information or account information to identify the customer. Where the password is not available, we follow the FCC guidelines by contacting the customer at either the telephone of record or by mailing the information to the address of record. In the case where the customer is able to provide call detail information during the customer-initiated call without our assistance, then we discuss the call detail information provided by the customer. In the case of an in-store visit, we verify the customer's identity by viewing a valid photo ID matching the customer's account information. In the event the ID does not match the account information, then we follow the procedures above by contacting

[1] Revised FCC rules effective December 8, 2007 of Section 64.2009

the customer at either the telephone of record or by mailing the information to the address of record.

(2) We have designed procedures for establishing passwords and back-up authentication without the use of readily available biographical information or account information. If the customer cannot provide the correct password or the correct response for the back-up authentication, then the customer is required to establish a new password and back-up authentication information.

(3) We notify customers immediately whenever a password, response to a back-up question for lost or forgotten passwords, or when an address of record is created or changed. The exception to this requirement is when the customer initiates service. We currently utilize the method of mailing notices to the address of record or initiating a voicemail to the telephone of record. The notices do not reveal the changed information and are not sent to the new account information.

(4) We do not make contractual agreements with business customers, therefore we do not exempt business customers from our methods of authentication.

Notifications of CPNI security breaches (§64-2011)

(1) [2]In the event a breach *(as used in this section, a "breach" has occurred when a person, without authorization of exceeding authorization, has intentionally gained access to, used, or disclosed CPNI)* has been determined, as soon as possible but no later than seven (7) business days after Company shall electronically notify the United States Secret Service (USSS) and the Federal Bureau of Investigation (FBI) through a central reporting facility. The Commission link for reporting will be maintained at http://www.fcc.gov/eb/cpni. In addition, Company will notify the Missouri Public Service Commission (MOPSC) of said breach. Company will not notify customer or disclose breach to the public until seven (7) full business days have passed after notification to the USSS, FBI, and the MOPSC.

(2) In the event we believe there is an extraordinarily urgent need to notify any class of affected customer sooner than otherwise allowed under paragraph (1) above, in order to avoid immediate and irreparable harm, we shall indicate it in our notification and will proceed to immediately notify the affected customer(s) only after consultation with the relevant investigating agency. We will cooperative with the relevant investigating agency's request to minimize any adverse effects of such customer notification.

(3) If the relevant investigating agency determines the public disclosure or notice to customer(s) would impede or compromise an ongoing or potential criminal investigation or national security, we may be directed not to disclose or notify for an initial period of up to 30 days. Such period may

[2] Revised FCC rules effective December 8, 2007 of Section 64.2011

be extended by the agency as reasonably necessary in the judgment of the agency. The agency shall provide in writing its initial direction, subsequent extensions, and any notifications that notice to customer will no longer impede or compromise a criminal investigation or national security.

(4) Only after we have completed the process in steps 1 through 3 above will we notify customers of the breach of that customer(s) CPNI.

(5) We will maintain a record, electronically or paper copy of any breaches discovered, notifications made to the USSS, the FBI and the MOPSC pursuant to these procedures, and notifications made to customers. The record will include, if available, date of discover and notification, a detailed description of the CPNI that was the subject of the breach, and the circumstances of the breach. We will maintain these records for a minimum of 2 years.

REVIEW AND REVISION OF PROCEDURES

We shall undertake the responsibility of reviewing these procedures on a continuing basis to ensure compliance with all Rules and Regulations regarding the utilization of CPNI. We shall revise these procedures on a timely basis to reflect any subsequent revisions to the applicable Rules and Regulations addressing CPNI.

Last Review date: 1-18-2010

Reviewed by: [illegible]

Title of Reviewer: Controller