Beacon
Telecommunications Advisors

8801 South Yale Avenue, Suite 450
Tulsa, Oklahoma 74137
Telephone 918.496.1444

www.beaconbright.com

February 8, 2010

Steelville Long Distance
P. O. Box 370
Steelville, MO 65565-0370

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

RE: EB Docket No. 06-36

Via: ECFS

Dear Secretary Dortch:

Pursuant to 47 C. F. R. § 64.2009(e); please find the accompanying annual CPNI certification and statement for calendar year 2009 for Steelville Long Distance form 499 filer ID number 819720.

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

Best Regards,

Keith Gile

Keith Gile
Consultant

Cc:
Byron McCoy, Telecommunications Consumer Division, Enforcement Bureau via email: byron.mccoy@fcc.gov

Best Copy Printing via email: fcc@bcpiweb.com

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

E B Docket 06-36

Annual 64.2009(e) CPNI Certification for 2009

Date Filed: February 8, 2010

Name of company covered by this certification: Steelville Long Distance

Form 499 Filer ID: 819720

Name of signatory: Donald R. Santhuff

Title of Signatory: General Manager

I, Donald R. Santhuff, 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 set forth in sections 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.

The company ~~has~~ not received any customer complaints in the past year concerning the unauthorized release of CPNI.

Signed _____

Steelville Long Distance (The Company)
STATEMENT OF COMPLIANCE WITH CPNI
47 U.S.C. §222, and 47 C.F.R. § 64.2001- 64.2011
EB Docket No. 06-36

The Company has established operating procedures that ensure compliance with Federal Communication Commission regulations regarding the protection of customer proprietary network information ("CPNI"). The Company maintains a CPNI policy manual that covers in detail the material summarized below.

CPNI Use

- The Company does not use or disclose CPNI without customer consent, except as permitted by 47 U.S.C. § 222 or 47 C.F.R. § 64.2005.
- The Company may use CPNI without customer consent to market communications-related services within those categories of service to which a customer already subscribes.
- The Company may use CPNI to market other communications-related services only after providing each customer with an opt-out notice via regular mail.
    - Customers may "opt out" of the use of CPNI described in the opt-out notice at any time via toll free number, email, regular mail, or business office visit.
    - The Company waits 33 days before assuming that a customer has consented to the use of CPNI described in the opt-out notice, provided that the customer has not already "opted out" of such use.
    - The Company records each customer's opt-out preference in the Company's automated information system, allowing the customer's opt-out consent status to be determined prior to use of CPNI.
    - The opt-out notice is refreshed every two years.
    - The Company provides written notice to the FCC, within five business days, of any instance where opt-out procedures do not work properly and to such a degree that the customer's inability to opt-out is more than an anomaly.
    - The Company requires supervisory review to ensure that any proposed uses of CPNI are covered by existing notices.
- The Company does not use or permit third parties to access CPNI for marketing purposes. As such, the Company generally does not seek opt-in consent from its customers.
- During customer-initiated telephone calls or business office visits, and following successful authentication, a customer may be asked to provide one time opt-in consent to allow the Company to use CPNI for marketing purposes during that call or visit.
- The Company requires sales personnel to obtain supervisory approval of all requests to use CPNI for outbound marketing, and maintains records of compliance for at least one year.

Authentication of Customer Identity

- The Company uses the procedures specified in 47 C.F.R. § 64.2010 to authenticate a customer's identity before sharing any CPNI with that customer.
- For in-person requests, the Company requires the customer to present a valid, government-issued photo ID.
- For telephone requests, the Company requires the customer to provide a password that is not prompted by a request for readily available biographical information, or account information. The company also uses a "hint" question and answer as a back-up means of authentication for each customer, which does not prompt the customer for readily available biographical information or account information.
- If the Company cannot authenticate the customer, the Company will release CPNI only by sending it to the customer's address of record, provided that it has been in effect for at least 30 days.

Training and Disciplinary Measures

- The Company has implemented internal procedures to educate and train new employees about proper and improper use of CPNI and the disclosure of CPNI.

- The Company has designated CPNI Compliance officer(s) that are responsible for the active monitoring, management and training of all employees with access to CPNI – including but not limited to customer service representatives.
- Employees are instructed to report each potential CPNI violation or breach to supervisors, and the Company has a process for documenting and investigating each potential violation or breach.
- The Company has established disciplinary procedures for any employee that wrongfully accesses, uses, or discloses CPNI, which explicitly state that employees can be terminated for failure to follow the Company's CPNI policies and comply with the Commission's CPNI rules.

Restricted Access to Records and Facilities

- The Company's automated information system, which contains the CPNI of the Company's customers, is password-protected.
    - Employees with access are required to lock their terminals before leaving their workstation unattended.
    - Supervisors are required to monitor employees for compliance with all system security measures.
- All physical facilities containing CPNI are secured, with restricted physical access.

Management of Potential CPNI Breaches and Law Enforcement Requests for CPNI

- Consistent with 47 C.F.R. § 64.2011, the company has adopted procedures for notifying law enforcement of CPNI breaches and providing deferred notification to customers.
- The Company maintains records of any and all potential CPNI breaches.
- The Company validates the authenticity of all requests from law enforcement, and ensures that such requests are lawful, before releasing CPNI.