KELLEY DRYE & WARREN LLP

A LIMITED LIABILITY PARTNERSHIP

WASHINGTON HARBOUR, SUITE 400

3050 K STREET, NW

WASHINGTON, D.C. 20007-5108

(202) 342-8400

NEW YORK, NY
LOS ANGELES, CA
CHICAGO, IL
STAMFORD, CT
PARSIPPANY, NJ

BRUSSELS, BELGIUM

AFFILIATE OFFICES
MUMBAI, INDIA

FACSIMILE
(202) 342-8451
www.kelleydrye.com

DENISE N. SMITH
DIRECT LINE: (202) 342-8614
EMAIL: dsmith@kelleydrye.com

February 29, 2016

VIA ECFS

Marlene H. Dortch
Secretary
Federal Communications Commission
445 12th Street, S.W.
Washington, DC 20554

Re: Annual Customer Proprietary Network Information Compliance Certification; EB Docket No. 06-36

Dear Ms. Dortch:

On behalf of DigitalSpeed Communications, Inc. ("DigitalSpeed") and pursuant to 47 C.F.R. § 64.2009(e), attached please find DigitalSpeed's 2016 Annual Customer Proprietary Network Information compliance certification covering calendar year 2015.

Please contact the undersigned at (202) 342-8614 if you have any questions regarding this filing.

Respectfully Submitted,

Denise N. Smith

Counsel to DigitalSpeed Communications, Inc.

Attachment

DIGITALSPEED COMMUNICATIONS, INC.

ANNUAL 47 C.F.R. § 64.2009(e) CPNI CERTIFICATION

EB DOCKET NO. 06-36

Annual Section 64.2009(e) CPNI Certification for 2016 covering the prior calendar year 2015.

Name of Company: DigitalSpeed Communications, Inc.

Form 499 Filer ID: 823686

Name of Signatory: Adam Pasternack

Title of Signatory: President

I, Adam Pasternack, certify that I am an officer of DigitalSpeed Communications, Inc. ("DigitalSpeed"), and acting as an agent of DigitalSpeed, that I have personal knowledge that DigitalSpeed has established operating procedures that are adequate to ensure compliance with the Federal Communications Commission's ("Commission" or "FCC") Customer Proprietary Network Information ("CPNI") rules. *See* 47 C.F.R. § 64.2001 *et seq.*

Attached to this certification is an accompanying statement explaining how DigitalSpeed's procedures ensure that it is in compliance with the requirements set forth in sections 64.2001 *et seq.* of the Commission's rules. *See* 47 C.F.R. § 64.2009(e).

DigitalSpeed has not taken any actions (*i.e.* instituted proceedings or filed petitions at either state commissions, the court system, or at the FCC) against data brokers during the above-referenced certification period. DigitalSpeed has no information outside of Commission Docket No. 96-115, or that is not otherwise publicly available (*e.g.,* through news media), regarding the processes pretexters are using to attempt to access CPNI. The steps that DigitalSpeed is taking to protect CPNI are described in the attached statement that summarizes DigitalSpeed's operating procedures for compliance with the Commission's CPNI rules.

DigitalSpeed has not received any customer complaints during the above-referenced certification period concerning the unauthorized release of CPNI.

Date: 02/26/16

Adam Pasternack
President
DigitalSpeed Communications, Inc.

STATEMENT REGARDING OPERATING PROCEDURES
IMPLEMENTING 47 C.F.R. SUBPART U
GOVERNING USE OF
CUSTOMER PROPRIETARY NETWORK INFORMATION ("CPNI")

DigitalSpeed Communications, Inc. ("DigitalSpeed") has established practices and procedures adequate to ensure compliance with Section 222 of the Communications Act of 1934, as amended, and the Federal Communications Commission's ("Commission's" or "FCC's") rules pertaining to customer proprietary network information ("CPNI") set forth in Sections 64.2001-64.2011 of the Commission's rules. This statement summarizes those practices and procedures.

Safeguarding against pretexting

- DigitalSpeed takes reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI, including the authentication of customers prior to disclosing CPNI based on customer-initiated contacts. DigitalSpeed is committed to notify the FCC of any novel or new methods of pretexting it discovers and of any actions it takes against pretexters and data brokers.

Training and discipline

- DigitalSpeed trains its supervisory and non-supervisory personnel in an effort to ensure that its employees, in accordance with FCC regulations: (a) understand what CPNI is; (b) join in and carry-out DigitalSpeed's obligation to protect CPNI; (c) understand when they are and when they are not authorized to use or disclose CPNI; (d) obtain customers' informed consent as required with respect to its use for marketing purposes; and (e) keep records regarding receipt of such consent, customer complaints regarding CPNI and the use of CPNI for marketing campaigns.

- DigitalSpeed employees are required to review DigitalSpeed's CPNI practices and procedures set forth in its training materials.

- DigitalSpeed also requires all outside Dealers and Agents to review DigitalSpeed's CPNI practices and procedures and to acknowledge receipt and review thereof.

- DigitalSpeed has an express disciplinary process in place for violation of the company's CPNI practices and procedures. The careless or intentional failure to comply with these practices and procedures may result in disciplinary action, up to and including discharge.

DigitalSpeed's use of CPNI

- DigitalSpeed may use CPNI for the following purposes:

  - To initiate, render, maintain, repair, bill and collect for services;
  - To protect its property rights; or to protect its subscribers or other carriers from fraudulent, abusive, or the unlawful use of, or subscription to, such services;
  - To provide inbound telemarketing, referral or administrative services to the customer during a customer initiated call and with the customer's informed consent;
  - To market additional services to customers that are within the same categories of service to which the customer already subscribes;
  - To market services formerly known as adjunct-to-basic services; and

- To market additional services to customers *with the receipt of informed consent via the use of opt-in or out-out, as applicable.*

- DigitalSpeed does not disclose or permit access to CPNI to track customers that call competing service providers.

- DigitalSpeed discloses and permits access to CPNI where required by law (*e.g.*, under a lawfully issued subpoena).

Customer approval and informed consent

- DigitalSpeed has implemented a system to obtain approval and informed consent from its customers prior to the use of CPNI for marketing purposes. This system also allows for the status of a customer's CPNI approval to be clearly established prior to the use of CPNI.

  - Prior to any solicitation for customer approval, DigitalSpeed notifies customers of their right to restrict the use of, disclosure of, and access to their CPNI.
  - DigitalSpeed uses opt-in approval when using or disclosing CPNI for purposes other than permitted under opt-out approval or in 47 U.S.C. § 222 and the FCC's CPNI rules.
  - A customer's approval or disapproval remains in effect until the customer revokes or limits such approval or disapproval.
  - Records of approvals are maintained for at least one year.
  - DigitalSpeed provides individual notice to customers when soliciting approval to use, disclose, or permit access to CPNI.
  - The content of DigitalSpeed's CPNI notices complies with Section 64.2008(c) of the FCC's rules.

Opt-out and Opt-Out

  - DigitalSpeed does not use CPNI for marketing purposes, nor does it disclose CPNI to third parties except where required by law.

One time use

  - After authentication, DigitalSpeed uses oral notice to obtain limited, one-time approval for use of CPNI for the duration of a call. The contents of such notice comports with Section 64.2008(f) of the FCC's rules.

Additional safeguards

- DigitalSpeed does not use CPNI for marketing purposes and therefore does not maintain records as required by Section 64.2009(c) of the FCC's rules. If this policy changes, DigitalSpeed will be sure to comply with all applicable regulations.

- DigitalSpeed designates one or more officers, as an agent or agents of the company, to sign and file a CPNI compliance certificate on an annual basis. The certificate conforms to the requirements set forth in Section 64.2009(e) of the FCC's rules.

- DigitalSpeed will provide written notice to the Commission in accordance with the requirements of Section 64.2009(f) of the FCC's rules if ever its opt-out mechanisms malfunction in the manner described therein.

- For customer-initiated telephone inquiries regarding or requiring access to CPNI, DigitalSpeed authenticates the customer (or its authorized representative), through a pre-established password, without prompting through the use of readily available biographical or account information. If the customer cannot provide a password, then DigitalSpeed only discloses call detail information by sending it to the customer's address of record, or by calling the customer at the telephone number of record.

- DigitalSpeed does not allow customers to access their CPNI online.

- DigitalSpeed notifies customers immediately of any account changes, including address of record, authentication, online account and password related changes.

- DigitalSpeed may negotiate alternative authentication procedures for services that DigitalSpeed provides to business customers that have both a dedicated account representative and a contract that specifically addresses DigitalSpeed's protection of CPNI.

- In the event of a breach of CPNI, DigitalSpeed will notify law enforcement as soon as practicable and no later than seven (7) business days from discovering the breach. As soon a practicable, and in no event later than seven (7) business days after reasonable determination of the breach, DigitalSpeed will electronically notify the U.S. Secret Service and Federal Bureau of Investigation through the central reporting facility at www.fcc.gov/eb/cpni. Customers will be notified after the seven (7) day period, unless the relevant investigatory party directs DigitalSpeed to delay notification, or DigitalSpeed and the investigatory party agree to an earlier notification. DigitalSpeed will maintain a record of all CPNI security breaches, including a description of the breach and the CPNI involved, along with notifications sent to law enforcement and affected customers.