Law Offices of Bennet & Bennet, PLLC

Maryland
4350 East West Highway, Suite 201
Bethesda, Maryland 20814
Tel: (202) 371-1500
Fax: (202) 371-1558
www.bennetlaw.com

District of Columbia
10 G Street NE, Suite 710
Washington, DC, 20002

Caressa D. Bennet
Michael R. Bennet
Gregory W. Whiteaker
Marjorie G. Spivak*
Donald L. Herman, Jr.
Kenneth C. Johnson‡
Howard S. Shapiro
Daryl A. Zakov⅄
Robert A. Silverman
Anthony K. Veach#

Of Counsel
Andrew Brown✧

*Admitted in DC & PA Only
‡Admitted in DC & VA Only
⅄Admitted in DC & WA Only
✧Admitted in DC & ME Only
#Admitted in DC & FL Only

January 20, 2011

Via ECFS

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

Re: CPNI Certification and Accompanying Statement
EB Docket No. 06-36

Dear Ms. Dortch:

Kaplan Telephone Company, Inc. ("the Company"), by its attorneys and pursuant to Section 64.2009(e) of the Commission's Rules, hereby submits its annual Customer Proprietary Network Information (CPNI) certification and accompanying statement.

Should you have any questions or need further information, please contact the undersigned.

Sincerely,

/s/ Marjorie Spivak

Marjorie Spivak

cc: Best Copy and Printing, Inc.

Attachments

CPNI Corporate Certification

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

EB Docket 06-36

Annual 64.2009(e) CPNI Certification for **2010**

Date filed: January **20, 2011**

Name of company(s) covered by this certification: Kaplan Telephone Company, Inc.

Form 499 Filer ID: 801054

Name of signatory: Carl A. Turnley

Title of signatory: Vice President

I, Carl A. Turnley, 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 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 Carl A. Turnley

Kaplan Telephone Company, Inc.
CPNI Usage Policy Statement

CPNI Policy Statement

Pursuant to Section 64.2009(e) of the Federal Communications Commission's ("FCC") rules, this statement explains how Kaplan Telephone Company, Inc.'s (the "Company") operating procedures ensure compliance with Part 64, Subpart U of the FCC's rules.

The Company has chosen to prohibit the use of CPNI for marketing purposes by itself and between its affiliates.

The Company policy manual includes an explanation of what CPNI is and when it may be used without customer approval.

Employees have been trained as to when they are and are not authorized to use CPNI. The Company policy manual describes the disciplinary process related to noncompliance with CPNI obligations, and sets forth the penalties for non-compliance, which can include termination of employment.

The Company has established a supervisory review process regarding Company compliance with the FCC's CPNI rules.

The Company requires affirmative written/electronic subscriber approval for the release of CPNI to third parties.

A Corporate Officer has been named as the CPNI Compliance Officer and is held responsible for annually certifying that the Company is in compliance with the FCC's CPNI rules and submitting the certification and an accompanying statement explaining how Company complies with the FCC's CPNI rules to the FCC prior to March 1.

Company Safeguards

The Company takes reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI. The Company has safeguards in place to protect against unauthorized access to CPNI. The Company authenticates a customer prior to disclosing CPNI based on customer initiated telephone contact or an in-store visit.

The Company only discloses call detail information over the telephone, based on customer-initiated telephone contact, if the customer first provides a password that is not prompted by the carrier asking for readily available biographical information or account information. If a customer does not provide a password, Company only discloses call detail information by sending it to an address of record or by calling the customer at the telephone of record. If the customer is able to provide call detail information during a

customer-initiated call without Company's assistance, then Company is permitted to discuss the call detail information provided by the customer.

The Company has established a system of passwords and password protection.
For a new customer (a customer that establishes service after the effective date of the new CPNI rules), Company requests that the customer establish a password at the time of service initiation. For existing customers to establish a password, Company must first authenticate the customer without the use of readily available biographical information or account information. Company authenticates a customer using non-public information such as calling the customer at the telephone number of record or using a Personal Identification Number (PIN) method to authenticate a customer.

For accounts that are password protected, Company cannot obtain the password by asking for readily available biographical information or account information to prompt the customer for his password. If a password is forgotten or lost, Company uses a back-up customer authentication method that is not based on readily available biographical information or account information.

If a customer does not want to establish a password, the customer may still access call detail based on a customer-initiated telephone call, by asking Company to send the call detail information to an address of record or by the carrier calling the telephone number of record.

Company does not currently provide online access to customers.

Company provides customers with access to CPNI at a carrier's retail location if the customer presents a valid photo ID and the valid photo ID matches the name on the account.

Company has procedures and policies in place to notify a customer immediately when a password, customer response to a back-up means of authentication for lost or forgotten passwords or address of record is created or changed.

In the event of a CPNI breach, Company complies with the FCC's rules regarding notice to law enforcement and customers. Company maintains records of any discovered breaches and notifications to the United States Secret Service (USSS) and the FBI regarding those breaches, as well as the USSS and the FBI responses to the notifications for a period of at least two year.

Actions Taken Against Data Brokers and Customer Complaints

Company has taken no actions against data brokers in the last year. Company has received no customer complaints in the past year concerning the unauthorized released of CPNI.