Kaplan Telephone Company, Inc.
Annual 47 CFR § 64.2009(e) CPNI Certification
EB Docket 06-36

Annual 64.2009(e) CPNI Certification for 2018 covering the prior calendar year 2017

1. Date filed: February 21, 2018

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

3. Form 499 Filer ID: 801054

4. Name of signatory: Carl A. Turnley

5. Title of signatory: Vice President

6. Certification:

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 CFR § 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 (including those mandating the adoption of CPNI procedures, training, safeguards, recordkeeping, and supervisory review) set forth in section 64.2001 *et seq.* of the Commission's rules.

The company has not taken actions (i.e., 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 customer complaints in the past year concerning the unauthorized release of CPNI.

The company represents and warrants that the above certification is consistent with 47 CFR § 1.17, which requires truthful and accurate statements to the Commission. The company also acknowledges that false statements and misrepresentations to the Commission are punishable under Title 18 of the U.S. Code and may subject it to enforcement action.

Signed Carl A. Turnley

Carl A. Turnley
Vice President
Kaplan Telephone Company, Inc.

Kaplan Telephone Company, Inc.

Explanation of Company Policies and Procedures
Regarding Compliance With CPNI Rules

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

Company CPNI Policies

The Company does not use CPNI for any purpose other than those specified in Section 64.2005 of the FCC's rules without customer consent. The Company has chosen to prohibit the use of CPNI for marketing purposes by itself and between its affiliates. In general, the Company does not share CPNI with third parties for marketing purposes or any other purpose that would require affirmative customer opt in consent.

The Company's CPNI Policy Manual includes an explanation of what CPNI is and when it may be used without customer approval.

Employees with access to CPNI have been trained as to when they are and are not authorized to use CPNI. The Company's CPNI 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 (except as authorized by proper documentation from a court or law enforcement).

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's CPNI 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, online account access, 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 or has chosen not to establish a password, Company only discloses call detail information by sending it to an address of record or by calling the customer at the telephone number of record. If the customer is able to provide call detail information during a customer-initiated call without Company's assistance, then Company discusses only the call detail information provided by the customer.

A customer may access call detail information by establishing a password protected online account or by visiting a carrier's retail location. The Company password protects online access to all CPNI, both call detail and non-call detail. 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.

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 a Personal Identification Number ("PIN") that has been provided to the customer at his address of record **[similar, but clarified]** or by calling the customer at the telephone number of record.

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.

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, online account, or address of record is created or changed.

Company has not experienced any CPNI-related security breaches in the past year. In the event of a CPNI breach, Company would notify law enforcement, as well as customers where appropriate, pursuant to Section 64.2011 of the FCC's rules. 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 years.

Actions Taken Against Data Brokers and Customer Complaints

Company has not taken any action against data brokers in the last year. Company has not received any customer complaints in the past year concerning the unauthorized released of CPNI.