ACCESS POINT INC.®
A TELECOMMUNICATIONS COMPANY

Received & Inspected

MAR 0 1 2016

FCC Mailroom

February 19, 2016
Via Electronic Filing

Ms. Marlene Dortch
Office of the Secretary
Federal Communications Commission
445 12th Street, SW
Washington, DC 20554

DOCKET FILE COPY ORIGINAL

RE: Access Point, Inc.
RE: Annual Certification of CPNI Filing March 1, 2016

Dear Ms. Dortch,

Enclosed please find the following e-filing of the ANNUAL 47 CFR Section §64.2009(e) CPNI Certification EB Docket 06-36. This certification is for the period since our last filing on March 1, 2015. The attachments include the Certification and an Accompanying Statement outlining the Access Point, Inc. operating procedures and compliance as required.

Please address any inquiries or further correspondence regarding this filing to my attention at (919) 851-4838 or to robin.byers@accesspointinc.com.

Sincerely,

Robin A. Byers
Chief Operating Officer

Enclosure

cc: Best Copy and Printing, Inc.
fcc@bcpiweb.com

No. of Copies rec'd 0
List ABCDE

ANNUAL 47 C.F.R. § 64.2009(e) CPNI Certification
EB Docket 06-36

Received & Inspected
MAR 01 2016
FCC Mailroom

Annual 64.2009(e) CPNI Certification for 2016

Date Filed: February 19, 2016

Name of Company covered by this certification: Access Point, Inc.

Name of Signatory: Robin A. Byers

Title of Signatory: Chief Operating Officer

I, Robin A. Byers, 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 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.

Signature

RE: Access Point, Inc.
RE: Annual 64.2009(e) CPNI Certificate for 2016

Accompanying Statement

This document comprises the Accompanying Statement to Access Point, Inc.'s Annual 64.2009 (e) CPNI Certificate for the year 2016. The purpose of this statement is to provide explanation as to how Access Point, Inc.'s operating procedures ensure compliance with the requirements set forth in section 64.2001 *et seq*. of the Commission's rules.

I. Operating Procedure Summary Description for; Section 64.2005 - Use of customer proprietary network information without customer approval.

The Access Point, Inc. operating procedure for use of CPNI without customer approval is that prior to the use of any customer's CPNI for any of the purposes stated in Section 64.2005, each customer whose CPNI is being contemplated for such use is checked individually in the company's customer record database, which contains an identifier field populated with the customer's CPNI status as either "Opt-in" or "Opt-out". All customer records contain this identifier. For any customers identified during this checking process as having an Opt-out status; the company then follows the rules and restrictions described in Section 64.2005 to determine if we may and how we may use their CPNI for the specific purpose intended. The checking process is conducted on individual customer records during the normal course of business and also for groups of customers of a certain class type prior to the start of a marketing campaign to that customer class type or as a system-wide audit report for management oversight purposes. This procedure is provided to employees in CPNI training seminars that are conducted on an ongoing basis and is overseen and reviewed by company management.

II. Operating Procedure Summary Description for Section 64.2007 Requirements [Approval required for use of customer proprietary network information.]

The Access Point, Inc. operating procedure for use of CPNI requiring customer approval is that prior to the use of any customer's CPNI for any of the purposes stated in Section 64.2007, each customer whose CPNI is being contemplated for such use is checked individually in the company's customer record database, which contains an identifier field populated with the customer's CPNI status as either "Opt-in" or "Opt-out". All customer records contain this identifier. For any customers identified during this checking process as having an Opt-out status; the company then follows the rules and restrictions described in Section 64.2005 to determine if we may and how we may use their CPNI for the specific purpose intended. The checking process is conducted on individual customer records during the normal course of business and also for groups of customers of a certain class type prior to the start of a marketing campaign to that customer class type or as a system-wide audit report for management oversight purposes. This procedure is provided to employees in CPNI training seminars that are conducted on an ongoing basis and is overseen and reviewed by company management.

III. Operating Procedure Summary Description for Section 64.2008 Requirements [Notice required for use of customer proprietary network information.]

The Access Point, Inc. operating procedure for providing notice for use of customer's CPNI is that we provide notice within our service contracts (Commercial Service Agreement, Residential Service Agreement) for every new or re-terming existing customer of their CPNI rights, our use and treatment of

their CPNI and instructions on how to opt-out from such use. Access Point, Inc. also provides notification messages on at least an annual basis to our customers, delivered to their address of record, reminding them of their CPNI rights, our use and treatment of their CPNI and instructions on how to opt-out from such continued use. The Opt-out procedure is available to our customers at any time via our public website and follows the requirements stated in 64.2008. The Opt-out procedures are provided to employees in CPNI training seminars that are conducted on an ongoing basis and are overseen and reviewed by company management.

IV. Operating Procedure Summary Description for Section 64.2009 Requirements [Safeguards required for use of customer proprietary network information.]

The Access Point, Inc. operating procedures for following and employing the Safeguards required for use of CPNI are described for each Safeguard individually;

1. The first Safeguard contained in 47CFR § 64.2009 is; (a) Telecommunications carriers must implement a system by which the status of a customer's CPNI approval can be clearly established prior to the use of CPNI.

Access Point, Inc. has implemented and maintains a system in which the status of a customer's CPNI approval is clearly established. This system consists of a CPNI Status data field that is populated in the main screen of each customer record in our electronic customer database. This data field displays the status of the customer's CPNI approval. The customer database, known as "CostGuard", is the desktop interface for all Access Point, Inc. employees' access to our customer records. By policy and process protocols each employee checks the status of each customer's CPNI approval in this data field prior to use of the CPNI. All employees have a unique login ID and password for accessing the customer database. The system tracks and records all data entries, including initial entries and change entries, to the CPNI Status data field. System reports are available to review all data entry activity. An audit is conducted by Access Point, Inc. management personnel on a regular basis to affirm that the CPNI Status data field for all Customers who have selected to opt-out properly matches our records of those notifications. Access Point, Inc. sales affiliates have restricted access to CPNI Status data fields for only the customers for which that they have sold Access Point, Inc. services. This access is via our "Partner Support Center", an internet portal that is firewall protected and restricted via individual user login ID and password combinations. Each sign-in event to the portal by an affiliate requires that they understand and comply with the policies and procedures regarding use and safeguarding of CPNI. The portal is linked to the CPNI status data field in the customer database. System reports are available to review all such data entry activity. Affiliates do not have data entry capabilities and are limited to "view-only" of the CPNI Status data field.

2. The second Safeguard contained in 47CFR § 64.2009 is; (b) Telecommunications carriers must train their personnel as to when they are and are not authorized to use CPNI, and carriers must have an express disciplinary process in place.

Access Point, Inc. provides training to its employees on authorized uses of CPNI, both to new employees at the time of hire as well as to the employee population on an ongoing basis. The company has established a written policy and processes for authorized use of CPNI. The policy is described in the company handbook, which is given to all employees at the time of hire and is published on the company's Intranet. The process documents are used during training on authorized use of CPNI and are published on the company's Intranet. The company also has established policy and procedures for processing requests from outside entities for its customer CPNI, including subpoena requests by government agencies. Access Point, Inc. has a specific disciplinary process in place for unauthorized use of CPNI, which is published in

the company handbook and is reviewed with each new employee at the time of hire and during subsequent training sessions.

3. The third Safeguard contained in 47CFR § 64.2009 is; (c) All carriers shall maintain a record, electronically or in some other manner, of their own and their affiliates' sales and marketing campaigns that use their customers' CPNI. All carriers shall maintain a record of all instances where CPNI was disclosed or provided to third parties, or where third parties were allowed access to CPNI. The record must include a description of each campaign, the specific CPNI that was used in the campaign, and what products and services were offered as a part of the campaign. Carriers shall retain the record for a minimum of one year.

Access Point, Inc. does maintain records, stored electronically as well as in paper form, of any and all of our own and our affiliates' sales and marketing campaigns that use our customers' CPNI and of all instances where CPNI was disclosed or provided to third parties, or where third parties were allowed access to CPNI for a period of no less than one year.

4. The fourth Safeguard contained in 47CFR § 64.2009 is; (d) Telecommunications carriers must establish a supervisory review process regarding carrier compliance with the rules in this subpart for outbound marketing situations and maintain records of carrier compliance for a minimum period of one year. Specifically, sales personnel must obtain supervisory approval of any proposed outbound marketing request for customer approval.

Access Point, Inc. has established a supervisory review process. We have created an oversight committee consisting of senior operating managers that reviews the policies, systems, databases, stored documents, processes and policies on an ongoing basis to determine that we are in compliance with the rules for outbound marketing situations and that we are maintaining records of compliance for a minimum period of one year.

5. The fifth Safeguard contained in 47CFR § 64.2009 is; (e) A telecommunications carrier must have an officer, as an agent of the carrier, sign a compliance certificate on an annual basis stating that the officer has personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the rules in this subpart. The carrier must provide a statement accompanying the certificate explaining how its operating procedures ensure that it is or is not in compliance with the rules in this subpart.

Access Point, Inc. is complying with 64.2009(e) herein.

6. The sixth Safeguard contained in 47CFR § 64.2009 is; (f) Carriers must provide written notice within five business days to the Commission 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.

(1) The notice shall be in the form of a letter, and shall include the carrier'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 the relevant state commission(s) has been notified and whether it has taken any action, a copy of the notice provided to customers, and contact information.

(2) Such notice must be submitted even if the carrier offers other methods by which consumers may opt-out.

Access Point, Inc. has had no instance where an opt-out mechanism did not work properly. However, if such an instance shall occur, the company will provide written notice within five business days to the Commission.

V. Operating Procedure Summary Description for Section 64.2010 Requirements [Safeguards on the disclosure of customer proprietary network information.]

1. The first Safeguard contained in 47CFR § 64.2010 is; (a) Safeguarding CPNI. Telecommunications carriers must take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI. Telecommunications carriers must properly authenticate a customer prior to disclosing CPNI based on customer initiated telephone contact, online account access, or an in-store visit.

The Access Point, Inc. operating procedure for discovering and protecting against attempts to gain unauthorized access to CPNI is to maintain password and firewall protection in all systems and databases containing CPNI, attain system reports and employee contact reports of unauthorized access attempts and to confirm that all requests for CPNI are by authenticated customers prior to providing access to , or disclosing CPNI during, either online access events or customer-initiated telephone calls. The company has no established retail locations or stores and provides no opportunities for in-store visits to our customers.

2. The second Safeguard contained in 47CFR § 64.2010 is; (b) Telephone access to CPNI. Telecommunications carriers may only disclose call detail information over the telephone, based on customer-initiated telephone contact, if the customer first provides the carrier with a password, as described in paragraph (e) of this section that is not prompted by the carrier asking for readily available biographical information, or account information. If the customer does not provide a password, the telecommunications carrier may only disclose call detail information by sending it to the customer's address of record, or, by calling the customer at the telephone number of record. If the customer is able to provide call detail information to the telecommunications carrier during a customer-initiated call without the telecommunications carrier's assistance, then the telecommunications carrier is permitted to discuss the call detail information provided by the customer.

The Access Point, Inc. operating procedure for disclosing call detail information over the telephone, based on customer-initiated telephone contact is; Employees request the password from the caller at the onset of all inbound calls requesting such information. For calls that the password has been provided correctly and authenticated, employees then commence to disclose call detail information over the telephone. On any call that the caller is unable to be authenticated through a password, the employee then declares to the caller that they can provide the requested call detail information only by either; sending it to the customer's address of record, or, by calling the customer at the telephone number of record or, by directing the customer to access their account online [requiring the use of the authenticated password by the customer]. The employee presents one or more of the three options to the customer based upon the information shown in the Costguard system that indicates which of the options are available to the customer at the time (i.e. An authenticated account password, a valid customer address of record exists, an authenticated password for on-line access exists, a valid telephone number of record exists). The procedures for disclosing call detail information over the telephone, based on customer-initiated telephone contact are provided to employees in CPNI training seminars that are conducted on an ongoing basis and are overseen and reviewed by company management.

3. The third Safeguard contained in 47CFR § 64.2010 is; (c) Online access to CPNI. A telecommunications carrier must authenticate a customer without the use of readily available biographical information, or account information, prior to allowing the customer online access to CPNI related to a telecommunications service account. Once authenticated, the customer may only obtain online access to CPNI related to a telecommunications service account through a password, as described in paragraph (e) of this section that is not prompted by the carrier asking for readily available biographical information, or account information.

The Access Point, Inc. operating procedure for authenticating a customer without the use of readily available biographical information, or account information, prior to allowing the customer online access to CPNI related to a telecommunications service account and once authenticated, ensuring that the customer may only obtain online access to CPNI related to a telecommunications service account through a password, as described in paragraph (e) of this section, that is not prompted by the carrier asking for readily available biographical information, or account information is to authenticate the customer prior to registering for electronic access, ensuring the electronic address of record has been on the customer's account for at least 30 days making it valid for use and for notification of account changes. The same authentication process is followed when establishing a new password.

4. The fourth Safeguard contained in 47CFR § 64.2010 is; (d) In-store access to CPNI. A telecommunications carrier may disclose CPNI to a customer who, at a carrier's retail location, first presents to the telecommunications carrier or its agent a valid photo ID matching the customer's account information.

Access Point, Inc. has no established retail locations or stores and provides no opportunities for in-store visits to our customers.

5. The fifth Safeguard contained in 47CFR § 64.2010 is; (e) Establishment of a Password and Back-up Authentication Methods for Lost or Forgotten Passwords. To establish a password, a telecommunications carrier must authenticate the customer without the use of readily available biographical information, or account information. Telecommunications carriers may create a back-up customer authentication method in the event of a lost or forgotten password, but such back-up customer authentication method may not prompt the customer for readily available biographical information, or account information. If a customer cannot provide the correct password or the correct response for the back-up customer authentication method, the customer must establish a new password as described in this paragraph.

The Access Point, Inc. operating procedure for establishment of a Password and Back-up Authentication Methods for Lost or Forgotten Passwords by authenticating the customer without the use of readily available biographical information, or account information and for creating a back-up customer authentication method in the event of a lost or forgotten password, but without prompting the customer for readily available biographical information, or account information is currently supported as follows; Customers can request a PIN be generated for their account through "Costguard". Costguard will generate a PIN to a valid address of record either through postal mail or electronic mail. Once received the customer can call back into the Access Point, Inc. customer service center and assign a password by authenticating themselves with the PIN. The procedures for disclosing call detail information over the telephone, based on customer-initiated telephone contact are provided to employees in CPNI training seminars that are conducted on an ongoing basis and are overseen and reviewed by company management.

6. The sixth Safeguard contained in 47CFR § 64.2010; (f) Notification of account changes. Telecommunications carriers must notify customers immediately whenever 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. This notification is not required when the customer initiates service, including the selection of a password at service initiation. This notification may be through a carrier-originated voicemail or text message to the telephone number of record, or by mail to the address of record, and must not reveal the changed information or be sent to the new account information.

The Access Point, Inc. operating procedure for notifying customers immediately whenever 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 is that all such events are conducted via customer-initiated telephone call or address of record validated email to our customer service department. Access Point, inc. does not currently provide any other methodologies or access paths to our customers to initiate or complete these activities. All such change requests are logged into the customer's account record and upon completion of the change, the employee who processed the change sends a notice to the address of record that a change has completed on the account. The notice form and content is in compliance with requirements of 64.2010. The notification of account changes procedure is provided to employees in CPNI training seminars that are conducted on an ongoing basis and is overseen and reviewed by company management.

VI. Operating Procedure Summary Description for Section 64.2011 Requirements [Notification of customer proprietary network information security breaches.]

The Access Point, Inc. operating procedure for notification of CPNI security breaches is that all employees are instructed to notify management immediately if they observe, discover or believe that a breach has occurred. Management will notify the Director of Customer Service who is then responsible for notifying law enforcement entity and the customer per the requirements of 64.2011. All instances of a breach event, as well as any resulting notifications are maintained in a log created for such purposes in the company's system. These records are maintained for a minimum of 2 years. The breach discovery, reporting and notification procedures are provided to employees in CPNI training seminars that are conducted on an ongoing basis and are overseen and reviewed by company management.