Palo
Cooperative Telephone
Association

February 1, 2016

BY ELECTRONIC FILING

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

RE: Certification of CPNI Filing (December 31, 2015)
EB-Docket No. 06-36

Dear Ms. Dortch:

In accordance with the Public Notice, DA 06-223, issued by the Enforcement Bureau on January 30, 2006, Palo Cooperative Telephone Association hereby files its most recent certification regarding its compliance with the rules of the Federal Communications Commission set forth in 47 C.F.R. Part 64, Subpart U.

If you have any questions, please feel free to contact me at 319-851-3431.

Sincerely,

Scott E Hobson

Scott Hobson
Compliance Officer

807 2nd St PO Box 169 Palo IA 52324 319-851-3431
www.palotelephone.com

Palo
Cooperative Telephone
Association

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

Annual 64.2009(e) CPNI Certification for 2015

1. Date filed: February 1, 2016
2. Name of company covered by this certification: Palo Cooperative Telephone Association
3. Form 499 Filer ID: 801171
4. Name of signatory: Scott Hobson
5. Title of signatory: Compliance Officer
6. Certification:

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

The company has not taken any 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 any 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. C.F.R. § 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.

Scott E Hobson

Scott Hobson
Compliance Officer

807 2nd St PO Box 169 Palo IA 52324 319-851-3431
www.palotelephone.com

Palo Cooperative Telephone Association
807 2nd Street
P.O. Box 169
Palo, Iowa 52324

Accompanying Statement

Palo Cooperative Telephone Association ("Company") maintains the following operating procedures to ensure compliance with the rules set forth in 47 C.F.R. Part 64, Subpart U:

Section 64.2005 Use of customer proprietary network information without customer approval.

(a) Any telecommunications carrier may use, disclose, or permit access to CPNI for the purpose of providing or marketing service offerings among the categories of service (i.e., local, interexchange, and CMRS) to which the customer already subscribes from the same carrier, without customer approval.

(1) If a telecommunications carrier provides different categories of service, and a customer subscribes to more than one category of service offered by the carrier, the carrier is permitted to share CPNI among the carrier's affiliated entities that provide a service offering to the customer.

(2) If a telecommunications carrier provides different categories of service, but a customer does not subscribe to more than one offering by the carrier, the carrier is not permitted to share CPNI with its affiliates, except as provided in §64.2007(b).

(b) A telecommunications carrier may not use, disclose, or permit access to CPNI to market to a customer service offerings that are within a category of service to which the subscriber does not already subscribe from that carrier, unless that carrier has customer approval to do so, except as described in paragraph(c) of this section.

(1) A wireless provider may use, disclose, or permit access to CPNI derived from its provision of CMRS, without customer approval, for the provision of CPE and information service(s). A wireline carrier may use, disclose or permit access to CPNI derived from its provision of local exchange service or interexchange service, without customer approval, for the provision of CPE and call answering, voice mail or messaging, voice storage and retrieval services, fax store and forward, and protocol conversion.

(2) A telecommunications carrier may not use, disclose, or permit access to CPNI to identify or track customers that call competing service providers. For example, a local exchange carrier may not use local service CPNI to track all customers that call local service competitors.

(c) A telecommunications carrier may use, disclose, or permit access to CPNI, without customer approval, as described in this paragraph (c).

(1) A telecommunications carrier may use, disclose, or permit access to CPNI, without customer approval, in its provision of inside wiring installation, maintenance, and repair services.

(2) CMRS providers may use, disclose, or permit access to CPNI for the purpose of conducting research on the health effects of CMRS.

(3) LECs, CMRS providers, and interconnected VoIP providers may use CPNI, without customer approval, to market services formerly known as adjunct-to-basic services, such as, but not limited to, speed

dialing, computer-provided directory assistance, call monitoring, call tracing, call blocking, call return, repeat dialing, call tracking, call waiting, caller I.D., call forwarding, and certain Centrex features.

(d) A telecommunications carrier may use, disclose, or permit access to CPNI to protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services.

The Company has adopted specific CPNI policies to ensure that, in the absence of customer approval, CPNI is only used by the Company to provide or market service offerings among the categories of service (i.e., local, interexchange, and CMRS) to which the customer already subscribes. The Company's CPNI policies prohibit the sharing of CPNI with affiliated companies, except as permitted under Rule 64.2005(a)(1) or with customer approval pursuant to Rule 64.2007(b). The only exceptions to these policies are as permitted under 47 U.S.C. § 222(d) and Rule 64.2005.

Section 64.2007 Approval required for use of customer proprietary network information.

(a) A telecommunications carrier may obtain approval through written, oral or electronic methods.

(1) A telecommunications carrier relying on oral approval shall bear the burden of demonstrating that such approval has been given in compliance with the Commission's rules in this part.

(2) Approval or disapproval to use, disclose, or permit access to a customer's CPNI obtained by a telecommunications carrier must remain in effect until the customer revokes or limits such approval or disapproval.

(3) A telecommunications carrier must maintain records of approval, whether oral, written or electronic, for at least one year.

In all circumstances where customer approval is required to use, disclose or permit access to CPNI, the Company's CPNI policies require that the Company obtain customer approval through written, oral or electronic methods in compliance with Rule 64.2007. A customer's approval or disapproval remains in effect until the customer revokes or limits the approval or disapproval. The Company maintains records of customer approval (whether written, oral or electronic) for a minimum of one year.

(b) *Use of Opt-Out and Opt-In Approval Processes*. A telecommunications carrier may, subject to opt-out approval or opt-in approval, use its customer's individually identifiable CPNI for the purpose of marketing communications-related services to that customer. A telecommunications carrier may, subject to opt-out approval or opt-in approval, disclose its customer's individually identifiable CPNI, for the purpose of marketing communications-related services to that customer, to its agents and its affiliates that provide communications-related services. A telecommunications carrier may also permit such person or entities to obtain access to such CPNI for such purposes. Except for use and disclosure of CPNI that is permitted without customer approval under section §64.2005, or that is described in this paragraph, or as otherwise provided in section 222 of the Communications Act of 1934, as amended, a telecommunications carrier may only use, disclose, or permit access to its customer's individually identifiable CPNI subject to opt-in approval.

The Company does not use CPNI for any purpose (including marketing communications-related services) and does not disclose or grant access to CPNI to any party (including to agents or affiliates that provide communications-related services), except as permitted under 47 U.S.C. § 222(d) and Rule 64.2005.

Section 64.2008 Notice required for use of customer proprietary network information.

(a) *Notification, Generally.* (1) Prior to any solicitation for customer approval, a telecommunications carrier must provide notification to the customer of the customer's right to restrict use of, disclose of, and access to that customer's CPNI.

(2) A telecommunications carrier must maintain records of notification, whether oral, written or electronic, for at least one year.

(b) Individual notice to customers must be provided when soliciting approval to use, disclose, or permit access to customers' CPNI.

(c) *Content of Notice.* Customer notification must provide sufficient information to enable the customer to make an informed decision as to whether to permit a carrier to use, disclose, or permit access to, the customer's CPNI.

(1) The notification must state that the customer has a right, and the carrier has a duty, under federal law, to protect the confidentiality of CPNI.

(2) The notification must specify the types of information that constitute CPNI and the specific entities that will receive the CPNI, describe the purposes for which CPNI will be used, and inform the customer of his or her right to disapprove those uses, and deny or withdraw access to CPNI at any time.

(3) The notification must advise the customer of the precise steps the customer must take in order to grant or deny access to CPNI, and must clearly state that a denial of approval will not affect the provision of any services to which the customer subscribes. However, carriers may provide a brief statement, in a clear and neutral language, describing consequences directly resulting from the lack of access to CPNI.

(4) The notification must be comprehensible and must not be misleading.

(5) If written notification is provided, the notice must be clearly legible, use sufficiently large type, and be placed in an area so as to be readily apparent to a customer.

(6) If any portion of a notification is translated into another language, then all portions of the notification must be translated into that language.

(7) A carrier may state in the notification that the customer's approval to use CPNI may enhance the carrier's ability to offer products and services tailored to the customer's needs. A carrier also may state in the notification that it may be compelled to disclose CPNI to any person upon affirmative written request by the customer.

(8) A carrier may not include in the notification any statement attempting to encourage a customer to freeze third-party access to CPNI.

(9) The notification must state that any approval, or denial of approval for the use of CPNI outside of the service to which the customer already subscribes from that carrier is valid until the customer affirmatively revokes or limits such approval or denial.

(10) A telecommunications carrier's solicitation for approval must be proximate to the notification of a customer's CPNI rights.

The Company's CPNI policies require that customers be notified of their rights, and the Company's obligations, with respect to CPNI prior to any solicitation for customer approval. All required customer notices (whether written, oral or electronic) comply with the requirements of Rule 64.2008. The Company maintains records of all required customer notices (whether written, oral or electronic) for a minimum of one year.

(d) *Notice Requirements Specific to Opt-Out.* A telecommunications carrier must provide notification to obtain opt-out approval through electronic or written methods, but not by oral communication (except as provided in paragraph (f) of this section). The contents of any such notification must comply with the requirements of paragraph (c) of this section.

(1) Carriers must wait a 30-day minimum period of time after giving customers notice and an opportunity to opt-out before assuming customer approval to use, disclose, or permit access to CPNI. A carrier may, in its discretion, provide for a longer period. Carriers must notify customers as to the applicable waiting period for a response before approval is assumed.

(i) In the case of an electronic form of notification, the waiting period shall begin to run from the date on which the notification was sent; and

(ii) In the case of notification by mail, the waiting period shall begin to run on the third day following the date that the notification was mailed.

(2) Carriers using the opt-out mechanism must provide notices to their customers every two years.

(3) Telecommunications carriers that use e-mail to provide opt-out notices must comply with the following requirements in addition to the requirements generally applicable to notification:

(i) Carriers must obtain express, verifiable, prior approval from consumers to send notices via e-mail regarding their service in general, or CPNI in particular;

(ii) Carriers must allow customers to reply directly to e-mails containing CPNI notices in order to opt-out;

(iii) Opt-out e-mail notices that are returned to the carrier as undeliverable must be sent to the customer in another form before carriers may consider the customer to have received notice;

(iv) Carriers that use e-mail to send CPNI notices must ensure that the subject line of the message clearly and accurately identifies the subject matter of the e-mail; and

(v) Telecommunications carriers must make available to every customer a method to opt-out that is of no additional cost to the customer and that is available 24 hours a day, seven days a week. Carriers may satisfy this requirement through a combination of methods, so long as all customers have the ability to opt-out at no cost and are able to effectuate that choice whenever they choose.

The Company does not currently solicit "opt out" customer approval for the use or disclosure of CPNI. The Company does not use CPNI for any purpose (including marketing communications-related services) and does not disclose or grant access to CPNI to any party (including to agents or affiliates that provide communications-related services), except as permitted under 47 U.S.C. § 222(d) and Rule 64.2005.

(e) *Notice Requirements Specific to Opt-In.* A telecommunications carrier may provide notification to obtain opt-in approval through oral, written, or electronic methods. The contents of any such notification must comply with the requirements of paragraph (c) of this section.

The Company does not currently solicit "opt in" customer approval for the use or disclosure of CPNI. The Company does not use, disclose or grant access to CPNI for any purpose, to any party or in any manner that would require a customer's "opt in" approval under the Commission's CPNI Rules.

(f) *Notice Requirements Specific to One-Time Use of CPNI.* (1) Carriers may use oral notice to obtain limited, one-time use of CPNI for inbound and outbound customer telephone contacts for the

duration of the call, regardless of whether carriers use opt-out or opt-in approval based on the nature of the contact.

(2) The contents of any such notification must comply with the requirements of paragraph (c) of this section, except that telecommunications carriers may omit any of the following notice provisions if not relevant to the limited use for which the carrier seeks CPNI:

(i) Carriers need not advise customers that if they have opted-out previously, no action is needed to maintain the opt-out election;

(ii) Carriers need not advise customers that they may share CPNI with their affiliates or third parties and need not name those entities, if the limited CPNI usage will not result in use by, or disclosure to, an affiliate or third party;

(iii) Carriers need not disclose the means by which a customer can deny or withdraw future access to CPNI, so long as carriers explain to customers that the scope of the approval the carrier seeks is limited to one-time use; and

(iv) Carriers may omit disclosure of the precise steps a customer must take in order to grant or deny access to CPNI, as long as the carrier clearly communicates that the customer can deny access to his CPNI for the call.

In instances where the Company seeks one-time customer approval for the use or disclosure of CPNI, the Company obtains such approval in accordance with the disclosures, methods and requirements contained in Rule 2008(f).

Section 64.2009 Safeguards required for use of customer proprietary network information.

(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.

The Company's billing system allows authorized company personnel to easily determine the status of a customer's CPNI approval on the customer account screen prior to the use or disclosure of CPNI.

(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.

The Company has established CPNI compliance policies that include employee training on restrictions on the use and disclosure of CPNI and required safeguards to protect against unauthorized use or disclosure of CPNI. Employees have signed that they understand the CPNI policies and a violation of those policies will result in disciplinary action.

(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.

The Company's CPNI policies require that all sales and marketing campaigns including those utilizing CPNI be recorded and kept on file for at least one year. Records are also maintained for disclosure or access to CPNI by third parties. The records include the required information listed in Rule 64.2009(c).

(d) Telecommunications carriers must establish a supervisory review process regarding carrier compliance with the rules in this subpart for out-bound 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 out-bound marketing request for customer approval.

The Company's CPNI policies require employees to obtain approval from the Company's CPNI Compliance Officer for all marketing campaigns, including those utilizing CPNI, prior to initiating the campaign. Record of the marketing campaigns, along with the appropriate supervisory approval is maintained for at least one year.

(e) A telecommunications carrier must have an officer, as an agent of the carrier, sign and file with the Commission a compliance certificate on an annual basis. The officer must state in the certification that he or she 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. In addition, the carrier must include an explanation of any actions taken against data brokers and a summary of all customer complaints received in the past year concerning the unauthorized release of CPNI. This filing must be made annually with the Enforcement Bureau on or before March 1 in EB Docket No. 06-36, for data pertaining to the previous calendar year.

The required officer certification, actions taken against data brokers and summary of customer complaint documents are included with this accompanying statement. The Company will file these documents on an annual basis on or before March 1 for data pertaining to the previous calendar year.

(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 problems(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.

The Company does not currently solicit "opt out" customer approval for the use or disclosure of CPNI.

Section 64.2010 Safeguards on the disclosure of customer proprietary network information.

(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 Company's CPNI policies and employee training include reasonable measures to discover and protect against activity that is indicative of pretexting and employees are instructed to notify the CPNI Compliance Officer if any such activity is suspected.

(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 Company's CPNI policies ensure that a customer is only able to access call detail information over the telephone in one of the ways listed in Rule 64.2010(b). If the customer cannot remember their password, they are prompted to answer a security question. Neither the password nor the security question are based on readily available biographical information or account information. Customer service representatives are instructed to authenticate customers over the telephone in all instances except in the case where the customer provides the call detail information without the assistance of the Company.

(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 Company's customers do not currently have access to their account online.

(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.

The Company's CPNI policies allow the Company to disclose call detail CPNI to the customer at a retail location after presenting a valid photo ID that matches the customer's account information.

(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 Company's CPNI policies allow for a few ways to establish a password, all of which ensure compliance with the above paragraph. Each method also allows the customer to establish a back-up or security question in the event that they forget their password. In no event does the Company use readily available biographical information or account information as a back-up question or as a means to establish a password or authenticate the customer.

(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 Company's billing system automatically generates a notification when any of the fields listed in Rule 64.2010(f) are created or changed. The Company then immediately notifies the customer through carrier-originated voicemail or text message to the telephone number of record, or by mail to the address of record (never a new address) when required by Rule 64.2010(f). The content of the notification complies with the requirements of Rule 64.2010(f).

(g) *Business Customer Exemption.* Telecommunications carriers may bind themselves contractually to authentication regimes other than those described in this section for services they provide to their business customer that have both a dedicated account representative and a contract that specifically addresses the carriers' protection of CPNI.

The Company does not utilize the business customer exception at this time.

Section 64.2011 Notification of customer proprietary network information security breaches.

(a) A telecommunications carrier shall notify law enforcement of a breach of its customers' CPNI as provided in this section. The carrier shall not notify its customers or disclose the breach publicly, whether voluntarily or under state or local law or these rules, until it has completed the process of notifying law enforcement pursuant to paragraph (b).

(b) As soon as practicable, and in no event later than seven (7) business days, after reasonable determination of the breach, the telecommunications carrier shall electronically notify the United States Secret Service (USSS) and the Federal Bureau of Investigation (FBI) through a central reporting facility. The Commission will maintain a link to the reporting facility at http://www.fcc.gov/eb/cpni.

(1) Notwithstanding any state law to the contrary, the carrier shall not notify customers or disclose the breach to the public until 7 full business days have passed after notification to the USSS and the FBI except as provided in paragraphs (2) and (3).

(2) If the carrier believes that there is an extraordinarily urgent need to notify any class of affected customers sooner than otherwise allowed under paragraph (1), in order to avoid immediate and irreparable harm, it shall so indicate in its notification and may proceed to immediately notify its affected customers only after consultation with the relevant investigating agency. The carrier shall cooperate with the relevant investigating agency's request to minimize any adverse effects of such customer notification.

(3) If the relevant investigating agency determines that the public disclosure or notice to customers would impede or compromise an ongoing or potential criminal investigation or national security, such agency may direct the carrier not to so disclose or notify for an initial period of up to 30 days. Such period may be extended by the agency as reasonable necessary in the judgment of the agency. If such direction is given, the agency shall notify the carrier when it appears that public disclosure or notice to affected customers will no longer impede or compromise a criminal investigation or national security. The agency shall provide in writing its initial direction to the carrier, any subsequent extension, and any notification that notice will no longer impede or compromise a criminal investigation or national security and such writings shall be contemporaneously logged on the same reporting facility that contains records of notifications filed by carriers.

(c) *Recordkeeping.* All carriers shall maintain a record, electronically or in some other manner, of any breaches discovered, notification made to the USSS and the FBI pursuant to paragraph (b), and notification made to customers. The record must include, if available, dates of discovery and notification, a detailed description of the CPNI that was the subject of the breach, and the circumstances of the breach. Carriers shall retain the record for a minimum of 2 years.

The Company has policies and procedures in place to ensure compliance with Rule 64.2011. When it is reasonably determined that a breach has occurred, the CPNI Compliance Officer will notify law enforcement and its customer in the required timeframes. A record of the breach will be maintained for a minimum of two years and will include all information required by Rule 64.2011.