ALPINE communications

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

EB Docket 06-36

Annual 64.2009(e) CPNI Certification for 2018

Date Filed: February 18, 2019

Name of Company(s) Covered by this Certification:

Company Name	Form 499 Filer ID
Alpine Long Distance, L.C.	816808

Name of Signatory: Chris Hopp

Title of Signatory: Chief Operating Officer

Certification:

I, Chris Hopp, acting as an agent of the company identified above, certify that I am an officer of the company and that I have personal knowledge that the company has established operating procedures that are adequate to ensure that the company is in compliance with the Commission's CPNI rules, including all requirements set forth in 47 C.F.R. § 64.2001 *et. seq.*

Attached to this certification is an accompanying statement explaining how the company's operating procedures ensure that the company is in compliance with the requirements (including those mandating the adoption of CPNI compliance policies and procedures, training, record keeping and supervisory review) set forth in 47 C.F.R. § 64.2001 *et. seq.*

The company has not taken any actions (either in proceedings instituted or petitions filed by the company with state commissions, the court system or the Commission) against data brokers in the past year.

The company has not received any customer complaints in the past year concerning the unauthorized, use, disclosure or 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 the company to enforcement action.

Name: Chris Hopp

Title: Chief Operating Officer

ACCOMPANYING STATEMENT

This statement accompanies the Annual 64.2009(e) CPNI Certification for 2018 filed with the Commission on behalf of Alpine Long Distance, L.C., an Iowa limited liability company (the "**Company**"). The Company's operating procedures ensure that the Company is in compliance with the requirements set forth in the Commission's CPNI rules as set forth in 47 C.F.R. Part 64, Subpart U (the "**CPNI Rules**") as follows:

- The Company has adopted operating procedures 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 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.

- In all circumstances where customer approval is required to use, disclose or permit access to CPNI, the Company's operating procedures 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. The Company's internal systems identify and permit authorized Company personnel to easily determine a customer's CPNI approval status at all times during customer interactions.

- Except as otherwise permitted under Rule 64.2005, the Company's CPNI policies require that the Company obtain a customer's "opt out" or "opt in" approval pursuant to Rule 64.2007(b) before the Company may use CPNI to market communications-related services or disclose CPNI to its agents or affiliates that provide communications-related services for marketing purposes. The Company does not use CPNI for any other purposes, and does not disclose or grant access to CPNI to any other party, except as permitted under 47 U.S.C. § 222(d) and Rule 64.2005.

- The Company's operating procedures 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.

- In instances where the Company is required to obtain customer approval for the use or disclosure of CPNI, the Company obtains "opt out" approval in accordance with the disclosures, methods and requirements contained in Rule 2008(c) and Rule 2008(d). The Company's CPNI policies require that Company provide "opt out" notices to its customers every two years. All customers have the ability to opt out at no cost and using methods that are available whenever the customer chooses. "Opt Out" notices were mailed to all Company customers with the November 2018 billing statements.

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

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

- The Company takes reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI. The Company's operating procedures include safeguards designed to identify and protect against unauthorized use, disclosure or 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 does not release call detail CPNI over the telephone, based on customer-initiated telephone contact, unless the customer first provides a password that is not prompted by the Company asking for readily available biographical information or account information or unless the customer is able to provide the relevant call detail information without Company assistance. If a customer does not provide a password and is not able to provide the relevant call detail information without Company assistance, the Company only discloses call detail CPNI by sending it to an address of record or by calling the customer at the telephone number of record.

- The Company provides customers with access to CPNI at the Company's retail locations only if the customer presents a valid photo ID and the valid photo ID matches the name on the customer account. If a customer is not able to provide a valid photo ID in connection with an in person inquiry, the Company only discloses call detail CPNI by sending it to an address of record or by calling the customer at the telephone number of record.

- The Company has established a system of passwords and password protection. For a new customer establishing service, the Company requests that the customer establish a password at the time of service initiation. For existing customers to establish a password, the Company must first authenticate the customer without the use of readily available biographical information or account information, for example by calling the customer at the telephone number of record or by using a personal identification number (PIN) or similar method to authenticate a customer.

- If a customer password is forgotten or lost, the Company uses a backup customer authentication method that is not based on readily available biographical information or account information. If a customer cannot provide a password or the proper response for the back-up authentication, the Company requires re-authentication of the customer.

- If a customer does not want to establish a password or if a password is lost or forgotten without subsequent authentication of the customer, the customer may only access call detail information based a customer-initiated telephone call by asking the Company to send the call detail information to an address of record or by the Company calling the customer at the telephone number of record.

- The Company provides online account access to customers. Online account access is password protected using a password established by the customer in the same manner and subject to the same restrictions as account passwords established for customer-initiated telephone contact. New and existing customers seeking online access to customer accounts are authenticated

without the use of readily available biographical information or account information, for example by using a personal identification number (PIN) or similar method to authenticate a customer. If a customer's online password is forgotten or lost, the Company uses a backup customer authentication method that is not based on readily available biographical information or account information. If a customer cannot provide a password or the proper response for the back-up authentication, the Company requires re-authentication of the customer.

- The Company has procedures and policies in place to notify a customer immediately when a password, customer response to a back-up means of authentication, address of record or other critical account information is created or changed.

- All Company employees with access to or a need to use CPNI have been trained regarding the Company's operating procedures and as to when they are and are not authorized to use, disclose or permit access to CPNI. The Company's employees have been trained regarding the types of information that constitute CPNI and the Company's safeguards (such as employee restrictions, password protection, supervisory review, etc.) applicable to the Company's handling of CPNI. The Company's employee manual describes the disciplinary process related to noncompliance with CPNI obligations and sets forth penalties for non-compliance, up to and including termination of employment. Company employees, including those in supervisory positions, monitor CPNI training opportunities and attend CPNI training events as appropriate.

- The Company has established a supervisory review process regarding the Company's compliance with the Commission's CPNI Rules for outbound marketing situations. The Company's marketing and sales personnel must obtain supervisory approval of any proposed outbound marketing request for customer CPNI approval. The Company maintains a record of its own and its affiliates' sales and marketing campaigns that use CPNI. The Company also maintains a record of all instances where CPNI was disclosed or provided to third parties and where third parties were permitted access to CPNI. Records of all sales and marketing campaigns involving CPNI, and of all instances where CPNI was disclosed or provided to third parties or where third parties were permitted access to CPNI, are maintained for a minimum of one year.

- The Company has appointed a compliance officer and established a supervisory review process regarding the Company's compliance with the Commission's CPNI Rules. The Company's operating policies require that employees confer with the compliance officer if they are unsure about any circumstances or situations involving the potential use, disclosure or release of CPNI. The Company's operating policies require that the compliance officer confer with the Company's legal counsel if he or she is unsure about any circumstances or situations involving the potential use, disclosure or release of CPNI.

- The Company's compliance officer has personal knowledge of the Company's operating procedures and is authorized, as an agent of the Company, to sign and file an annual CPNI compliance certification with the Commission.

- All Company employees and the compliance officer are trained to identify and protect against activity that is indicative of pretexting. All Company employees and the compliance officer are required to report any breach or potential breach of CPNI safeguards and/or any customer complaints regarding CPNI. In the event of a CPNI breach, the Company's operating procedures require compliance with the Commission's CPNI Rules regarding notice to law enforcement and

customers. The Company must maintain records of any discovered breaches and notifications to the Secret Service and the FBI regarding those breaches, as well as the Secret Service and the FBI responses to such notifications, for a period of at least two years.