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

EB Docket 06-36

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

Annual 64.2009(e) CPNI Certification for 2015

Date filed: February 1, 2016

Name of company(s) covered by this certification:
Polar Communications Mutual Aid Corp., Polar Telcom Inc., Wolverton Telephone Co.

Form 499 Filer ID: 804486, 821498, 801093

Name of signatory: David L. Dunning

Title of signatory: General Manager/CEO, Executive Vice President

I, David L. Dunning, certify that I am an officer of the companies named above, and acting as an agent of the companies, that I have personal knowledge that the companies have 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 companies' procedures ensure that the companies are in compliance with the requirements set forth in section 64.2001 *et seq.* of the Commission's rules.

The companies have 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 companies have 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 _____

Attachment

CC: Best Copy and Printing, Inc.
FCC@BCPIWEB.com

PO Box 270
110 4th Street East
Park River, ND 58270
701.284.7221
www.thinkpolar.com

POLAR

Statement of Compliance Procedures for CPNI

The operating procedures of Polar Communications Mutual Aid Corp., Polar Telcom Inc., and Wolverton Telephone Company are designed to ensure compliance with the CPNI rules applicable to them. Such procedures are as follows.

CPNI Use

(1) We use, disclose or permit access to CPNI to protect our rights and property, our Customers, and other carriers from fraudulent, abusive or unlawful use of, or subscription to, our services.
(2) We use, disclose or permit access to CPNI to provide or market service offerings to which the Customer already subscribes. When we provide different categories of service, and a Customer subscribes to more than one service category, we share the Customer's CPNI with the affiliate that provides service to the Customer; but if a Customer subscribes to only one service category, we do not share the customer's CPNI with an affiliate without the Customer's approval.
(3) We do not use, disclose or permit access to CPNI to identify or track Customers that call competing service providers.

CPNI Approvals

(1) When Customer approval to use, disclose or permit access to Customer CPNI is required, we obtain approval through written, oral or electronic method. We maintain all records for at least one year.
(2) Subject to "opt-out" approval requirements, we use a Customer's individually identifiable CPNI to market communications-related services to that Customer, and we disclose that CPNI to our affiliates that provide communications-related services. We also allow these to obtain access to such CPNI to market communications-related services.

CPNI Notice Requirements

(1) We individually notify and inform each Customer of his or her right to restrict the use or disclosure of, and access to, CPNI along with a solicitation of approval, and we maintain records of that notification, whether oral or written, for at least one year.
(2) Our notifications provide information sufficient to enable our Customers to make informed decisions as to whether to permit the use or disclosure of, or access to, their CPNI.
(3) We advise the Customer of the precise steps the Customer must take in order to grant or deny access to CPNI, and we clearly state that a denial of approval will not affect the provision of any services to which the Customer subscribes.
(4) Our notifications are comprehensible, not misleading, legible, and placed in an area readily apparent to the Customer.
(5) We do not include in the notification any statement that attempts to encourage a Customer to freeze third-party access to CPNI.
(6) For "opt-out" approvals, our notifications satisfy (1) – (5).
(7) In addition, for "opt-out" approvals, we provide notices to our customers every two years, and we make available to every customer a method to opt-out that is of no additional cost to the Customer and is available 24 hours a day, seven days a week. We may satisfy this requirement through a combination of methods, but we allow Customers to opt-out at no cost and whenever they choose.

Statement of Compliance Procedures for CPNI

CPNI Safeguards

(1) We have implemented a system by which the status of a Customer's CPNI approval can be clearly established prior to the use of the CPNI.
(2) We have a designated compliance officer to maintain and secure the company's CPNI records and to supervise training of all company employees.
(3) We have trained our personnel as to when they are, and are not, authorized to use CPNI, and we have an express disciplinary process in place to deal with employee failures.
(4) We authenticate the identity of a customer prior to disclosing CPNI based on a customer-initiated telephone contact, online account access, or in-store visit.
(5) We do not disclose call detail information over the phone.
(6) We disclose CPNI to a customer in person at our retail locations only when the customer presents a valid photo ID and the ID matches the name on the account.
(7) We notify a customer immediately of changes in: a customer's response to back-up means of authentication, online account, or address of record.
(8) We maintain a record of our own and our affiliates' sales and marketing campaigns that use Customers' CPNI. The record includes a description of each campaign, the specific CPNI that was used in the campaign, and what products and services were offered as part of the campaign. We retain these records for at least one year.
(9) We have established a supervisory review process regarding compliance with the CPNI rules for outbound marketing situations and we maintain compliance records for at least one year. Specifically, our sales personnel obtain supervisory approval of any proposed outbound marketing request for customer approval of the use of CPNI.
(10) We have a corporate officer who acts as agent for the Company and signs a compliance certificate on an annual basis stating that the officer has personal knowledge that the Company has established operating procedures adequate to ensure compliance with applicable CPNI rules. We provide a Statement accompanying the Certificate that explains our operating procedures and demonstrates compliance with the CPNI rules.
(11) We are prepared to provide written notice within five business days to the FCC 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.
(12) We are prepared to notify the U.S. Secret Service and FBI within seven business days after the occurrence of an intentional, unauthorized (or exceeding authorization), access to, use of, or disclosure of CPNI. We may also notify the customer of such breach, after consulting with the investigatory agency(ies), if we believe there is an extraordinary urgent need to notify a customer (or class of customers) in order to avoid immediate or irreparable harm. We will notify the customer of the breach after 7 business days following notification to the FBI and Secret Service, if such agencies have not requested that we postpone disclosure to the customer.
(13) We will maintain records of any discovered breaches, notices to the Secret Service and FBI, and their responses, for at least two years.

CPNI Statements

There were no events of unauthorized access to and/or distribution of our customer records by data brokers.
There were no customer complaints received in the past year concerning the unauthorized release of CPNI.