

## **STATEMENT OF COMPLIANCE**

The operating procedures of Crosslake Telephone Company d/b/a Crosslake Communications ensure compliance with the FCC's CPNI Rules. Such procedures are as follows:

### ***Use of CPNI in Marketing***

Our company does not use CPNI in any of its marketing efforts, and does not permit the use of, or access to, customer CPNI by our affiliates or any third parties. We use, disclose or permit access to CPNI only for the purposes permitted under 47 U.S.C. Sections 222(c)(1) and (d).

### ***CPNI Safeguards***

Our company has designated a compliance officer to maintain and secure the company's CPNI records and to supervise training of all company employees.

Our company trains its personnel as to when they are, and are not, authorized to use or disclose CPNI, and we have an express disciplinary process in place if the rules are violated.

Our company authenticates the identity of a customer prior to disclosing CPNI based on a customer-initiated telephone contact, online account access, or in-store visit.

Our company discloses call detail information (CDI) in a customer-initiated call only: after the customer provides a pre-established password; or, at the customer's request, by sending the CDI to the customer's address of record; or by calling back the customer at his or her telephone number of records.

Our company discloses CPNI to a customer in person at our retail location(s) only when the customer presents a valid photo ID and the ID matches the name on the account.

Our company establishes passwords with customers in order to authenticate customers. Neither passwords nor the backup method for authentication rely on customers' readily available biographical information.

Our company notifies a customer immediately of changes in: a customer's password, a customer's response to back-up means of authentication, online account, or address of record.

### ***CPNI Recordkeeping and Reporting***

Our company maintains records of our compliance with the FCC's CPNI Rules for use of CPNI in outbound marketing efforts, for at least one year.

Our company is prepared to provide the FCC with written notice, within five business days of any instance where the "opt out" mechanisms do not work properly.

Our company is 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 extraordinarily 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.

Our company will maintain records of any discovered breaches, notices to the Secret Service and FBI, and their responses, for at least two years.