

SIERRA TEL LONG DISTANCE

STATEMENT EXPLAINING HOW SIERRA TEL LONG DISTANCE'S OPERATING PROCEDURES ENSURE COMPLIANCE WITH THE FCC'S CPNI RULES

I. Definition of Customer Proprietary Network Information (CPNI)

Customer Proprietary Network Information or CPNI, is defined in Section 222(h) of the Communications Act to include any (A) information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and (B) information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier; except that such term does not include subscriber list information.

Call detail information is a category of CPNI that is particularly sensitive from a privacy standpoint and that is sometimes sought by pretexters, hackers, and other unauthorized individuals or entities for illegitimate and/or illegal purposes. Call detail includes any information that pertains to the transmission of a specific telephone call, including the number called (for outbound calls), the number from which the call was placed (for inbound calls), and the date, time, location and/or duration of the call (for all calls).

The Federal Communications Commission's (FCC's) CPNI Rules are articulated in a series of FCC orders, and summarized in 47 C.F.R. Section 64.2001, *et seq.* Sierra Tel Long Distance (STLD) has familiarized itself with these rules, including the definitions of "CPNI" and "call detail" presented above.

II. STLD Understands the Importance of Protecting CPNI, and Has Taken Steps to Ensure that Customers' CPNI Remains Secure and Confidential

STLD recognizes that CPNI includes information that is personal and individually-identifiable, and STLD understands that privacy concerns have led Congress and the FCC to impose restrictions upon its use and disclosure, and upon the provision of or access to CPNI by individuals or entities inside and outside STLD. STLD has implemented procedures that will preserve the confidentiality of this information, and STLD has taken steps to ensure that it is in compliance with the FCC's CPNI Rules.

III. STLD's CPNI Compliance Officer and the CPNI/Privacy Team

STLD has designated a CPNI Compliance Officer who is responsible for: (a) communicating with STLD's attorneys and/or consultants regarding CPNI responsibilities, requirements, and restrictions; (b) supervising the training of STLD employees and agents who use or have access to CPNI; (c) supervising the use, disclosure, distribution and/or access to STLD CPNI by independent contractors; (d) maintaining records regarding the use of CPNI in

marketing campaigns; and (e) receiving, reviewing, and resolving questions or issues regarding use, disclosure, distribution, and/or provision of access to CPNI.

STLD's primary CPNI Compliance Officer is the Customer Care Manager and, in his absence or as directed by the primary Compliance Officer, the Customer Care Supervisor is the alternate Compliance Officer.

In addition to the specific matters required to be reviewed and approved by STLD's CPNI Compliance Officer, employees are strongly encouraged to bring any and all other questions, issues, or uncertainties regarding the use, disclosure, and/or access to CPNI to the attention of STLD's CPNI Compliance Officer for appropriate investigation, review, and guidance. As discussed further below, the extent to which a particular employee or agent brings a CPNI matter to the attention of the CPNI Compliance Officer and receives appropriate guidance is a material consideration in any disciplinary action brought against the employee or agent for impermissible use, disclosure, or access to CPNI.

STLD has also developed a CPNI Privacy Team that is comprised of members of Customer Care, Regulatory, Billing, and Information Services Departments. This team works together to ensure that all CPNI requirements are met. There is an internal email address in place that distributes CPNI-related inquiries to the CPNI Compliance Officer, alternate CPNI Compliance Officer, Vice President Operations, Operations Manager, and the Regulatory Manager. This email address is for use by any and all employees so that they can send questions or information for review and guidance regarding CPNI issues, should they arise.

STLD takes reasonable measures to discover and protect against activity that is indicative of pretexting, including requiring STLD employees to notify the CPNI Compliance Officer immediately by voice, voicemail, or email of any suspicious activity that may suggest that someone is attempting to gain unauthorized access to a customer's CPNI.

IV. STLD's Policy Governing Use and Disclosure of CPNI

During 2011, STLD changed its procedure for use of CPNI. STLD had previously limited its use and disclosure of CPNI to marketing under the "total services approach," as described in 47 C.F.R. Section 64.2005 and to the types of uses that are recognized as exceptions to the opt-in and opt-out requirements under the federal CPNI rules. STLD is an affiliate of Sierra Telephone and calls made using STLD as a carrier appear only on Sierra Telephone bills. STLD adopted Sierra Telephone's procedure change from a "total services approach" to an "opt-out approval approach" as defined in 47 C.F.R. Section 64.2003. Following the guidelines in 47 C.F.R. Section 64.2007, Sierra Telephone sent opt-out notifications to all customers during its September 15, 2011 and October 1, 2011 bill cycle. Sierra Telephone and STLD waited the required minimum 33 days from the October 1, 2011 notification before implementing procedures in accordance with the "opt-out approval approach." For customers who chose to opt out from Sierra Telephone, STLD acknowledges the opt-out status for STLD.

Sierra Telephone, following the requirements listed in 47 C.F.R. Section 64.2008, mailed opt-out notices to customers that had not previously opted-out on September 15, 2015. For customers who chose to opt out from Sierra Telephone, STLD acknowledges the opt-out status for STLD.

STLD's employees and billing agents may use CPNI to initiate, render, bill, and collect for telecommunications services. STLD may obtain information from new or existing customers that may constitute CPNI as part of applications or requests for new, additional, or modified services, and its employees and agents may use such customer information to initiate and provide the services. Pursuant to established exceptions under the FCC's CPNI Rules, STLD's employees and billing agents may use customer service and calling records: (a) to bill customers for services rendered to them; (b) to investigate and resolve disputes with customers regarding their bills; and (c) to pursue legal, arbitration, or other processes to collect late or unpaid bills from customers.

STLD's employees and agents may use CPNI without customer approval to protect STLD's rights or property, and to protect users and other carriers from fraudulent, abusive, or illegal uses of (or subscription to) telecommunication service from which the CPNI is derived. Because allegations and investigations of fraud, abuse, and illegal use of CPNI constitute very sensitive matters, any access, use, disclosure, or distribution of CPNI pursuant to this Section must be expressly approved in advance and in writing by STLD's CPNI Compliance Officer.

V. Procedures for Customers to Obtain Access to CPNI

STLD's policy is to disclose or release call detail information to a customer during customer-initiated telephone contacts only when the customer has been properly authenticated and has provided a pre-established password. Passwords and shared secret questions and answers are designed in a manner that is privately significant and memorable to the customer, but they are not based upon readily obtainable biographical information. If the customer does not provide a password (or correct answers to the shared secret questions and answers), call detail information is released only by sending it to the customer's address of record (defined as the address that has been associated with the customer's account for at least 30 days), or by calling the customer at the telephone number of record (defined as the telephone number associated with the underlying service). As an additional protection to STLD's customers that goes beyond the requirements of the CPNI rules, employees authenticate all telephone requests for CPNI in the same manner whether or not the CPNI consists of call detail information.

STLD retains all customer passwords and shared secret questions and answers in secure files that may be accessed only by authorized company employees who need such information to authenticate the identity of customers requesting call detail information over the telephone.

A customer of record (*i.e.*, a customer whose name is on the account) may review and/or obtain copies of his or her CPNI at any Business Office or retail sales location where such CPNI is available by coming in-person to the facility and presenting a valid photo ID, such as a United States (U.S.) driver's license, U.S. passport, or other U.S. government-issued identification that verifies his or her identity, and matches the customer's account information.

STLD may, after receiving an appropriate written request from a customer, disclose or provide the customer's CPNI to the customer by sending it to the customer's address of record. Any and all such customer requests of this sort must be made in writing, and must: (a) include the customer's correct billing name, address, and telephone number; (b) specify exactly what type or types of CPNI are to be disclosed or provided; (c) specify the time period for which the CPNI must be disclosed or provided; and (d) be signed by the customer.

Customers may obtain an initial or replacement password if they: (a) come in-person to the Business Office, produce a U.S. driver's license, U.S. passport, or other U.S. government-issued identification verifying their identity with a valid photo ID, and correctly answer certain questions regarding their service and address of record; and/or if they (b) call the Business Office and the Customer Care Representative calls them back at the telephone number of record and obtains correct answers to certain questions regarding their service and address.

VI. Customer Notification of Account Changes

STLD has notified customers immediately of certain changes in their accounts that may affect privacy or security matters. The types of changes that require immediate notification include: (a) a change or request for change of the customer's password; (b) a change or request for change of the customer's address of record; (c) a change or request for change of any significant element of the customer's online account; and (d) a change or request for change to the customer's responses that constitute the back-up means of authentication for lost or forgotten passwords. Any of the above changes automatically produces a notice to the address of record.

The notice is provided by a written notice mailed to the customer's address of record. The notice is mailed to the customer's prior address of record if the change includes a change in the customer's address of record.

VII. Data Security Procedures for Protecting CPNI

Electronic files and databases containing CPNI are maintained on computers that are not accessible from the Internet or that are on the corporate Intranet behind firewalls that are regularly monitored, tested, and audited for effectiveness. In addition, such electronic files and databases may be accessed only by authorized STLD employees who have been authenticated by providing a unique login ID and password. STLD policy mandates that files containing CPNI be maintained in a secure manner such that they cannot be used,

accessed, disclosed, or distributed by unauthorized individuals or in an unauthorized manner. Paper files containing CPNI are kept in secure areas, and may not be used, removed, or copied without specific, prior authorization from a supervisor and/or the CPNI Compliance Officer. STLD employees are required to notify the CPNI Compliance Officer of any access or security problems they encounter with respect to files containing CPNI.

VIII. Law Enforcement Requests for CPNI and Reporting of Unauthorized Disclosures

STLD will provide a customer's telephone records or other CPNI to a law enforcement agency in accordance with applicable legal requirements. STLD employees are required to direct all law enforcement requests for CPNI (whether or not accompanied by a warrant or subpoena) to the CPNI Compliance Officer, who is responsible for handling such requests and for consulting with counsel as necessary.

STLD provides an initial notice to law enforcement and a subsequent notice to the customer if a security breach results in the disclosure of the customer's CPNI to a third party without the customer's authorization. As soon as practicable (and in no event more than seven (7) days) after STLD discovers that a person (without authorization or exceeding authorization) has intentionally gained access to, used, or disclosed CPNI. STLD must provide electronic notification of such a breach to the United States Secret Service (USSS) and to the Federal Bureau of Investigation (FBI) via a central reporting facility accessed through the following link maintained by the FCC: <http://www.fcc.gov/eb/cpni/Report.html>. STLD will notify the customer and/or disclose the breach publicly after seven business days following notification to the USSS and the FBI, if the USSS and the FBI have not requested that the telecommunications carrier continue to postpone disclosure.

IX. CPNI Employee Training

STLD employees who work with CPNI have been informed that there are substantial federal restrictions upon CPNI use, distribution, and access. In order to be authorized to use or access STLD's CPNI, employees received training with respect to the requirements of Section 222 of the Communications Act and the FCC's CPNI Rules.

On-site comprehensive training was provided for all employees in December 2007 regarding protection of CPNI, other types of confidential subscriber information, and otherwise protected information. The training also defined and provided detail information and examples of the "total services approach." The training was provided by corporate attorney, Patrick Rosvall, of Cooper, White and Cooper, LLP, with assistance from the CPNI/Privacy Team. Mr. Rosvall provided three different tiers of training: (a) general training sessions; (b) intensive training for employees with customer contact and employees who have access to customer records; and (c) management training for all managers and supervisors. These training sessions were recorded, and the training was reviewed by employees who were unable to attend on the original training dates. These recordings also were utilized for training of new employees, annual review, and recertification.

In conjunction with STLD's 2011 adoption of the "opt-out approval approach", STLD's CPNI Compliance Officer developed and presented new CPNI training for the "opt-out approval approach" to all employees, in accordance to C.F.R. Section 64.2009. The new training session was recorded for training of new employees, annual review, and recertification.

Upon completion of these annual training sessions, each employee signs a Certificate of Attendance and Acknowledgement of Duty to Protect Customer Proprietary Network Information and Other Protected Information. STLD retains these certificates in each employee's personnel records.

STLD has a comprehensive CPNI manual detailing the elements of its compliance with the federal CPNI rules, and setting forth its policies for handling CPNI and other confidential subscriber information.

X. Employee Disciplinary Procedures

STLD has informed its employees, agents, and independent contractors that it considers compliance with the Communications Act and FCC Rules regarding the use, disclosure, and access to CPNI to be very important. Violation by STLD employees or agents of such CPNI requirements will lead to disciplinary action up to and including remedial training, reprimands, unfavorable performance reviews, probation, and termination. Discipline in a given situation will depend upon the circumstances of the violation or violations, including the severity of the violation, whether the violation was a first time or repeat violation, whether appropriate guidance was sought or received from the CPNI Compliance Officer, and the extent to which the violation was or was not deliberate or malicious.