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

Annual 64.2009(e) CPNI Certification for: 2007

Company Names: SCS Communications & Security, Inc.

Address: 502 N 2nd Ave
Stayton, OR, 97383

Form 499 Filer ID: 820276

As a corporate officer of the Company, I hereby certify that, based on my personal knowledge, the Company has established operating and employee training procedures that are adequate to ensure compliance with the rules established by the Federal Communications Commission ("FCC") concerning Customer Proprietary Network Information" ("CPNI"), as set forth in Part 64, Subpart U, of the FCC's Rules and Regulations, 47 C.F.R. § 64.2001 *et seq.*, as revised.

The attached Statement explains how the Company's procedures ensure that the Company is in compliance with the requirements set forth in section 64.2001 *et seq.* of the Commission's rules.

The Company has not taken any actions against data brokers in the past year. The Company must report on any information that they have with respect to the processes pretexters are using to attempt to access CPNI, and what steps the Company is taking to protect CPNI.

The Company has not received any customer complaints in the past year concerning the unauthorized release of CPNI.

Marilyn Kendall
Printed Name of Signatory

Marilyn Kendall
Secretary / Treasurer

Dated: 2/5/08

Attachment

STATEMENT

The operating procedures of Stayton Cooperative Telephone Company, People's Telephone Co. and SCS Communications & Security, Inc. 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 among the categories of service - local, interexchange and CMRS -- 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 use, disclose or permit access to CPNI derived from our provision of CMRS for the provision of Customer Premises Equipment (CPE) and information services, without Customer approval.
(4) We use, disclose or permit access to CPNI derived from our provision of local exchange or interexchange service for the provision of CPE and call answering, voice mail or messaging, voice storage and retrieval services, fax store and - forward, and protocol conversion, without Customer approval.
(5) Without Customer approval, we do not use, disclose or permit access to CPNI to provide or market service offerings within a category of service to which the Customer does not already subscribe, except that we use, disclose or permit access to CPNI to: (a) provide inside wiring installation, maintenance and repair services; (b) conduct, when we provide CMRS, research on the health effects of CMRS; and (c) market, when we provide local service or CMRS, services formerly known as adjunct-to-basic services such as, but not limited to, speed dialing, computer-provided directory assistance, all monitoring, call tracing, call blocking, call return, repeat dialing, call tracking, call waiting, caller ID, call forwarding, and certain Centrex features.
(6) We do not use, disclose or permit access to CPNI to identify or track Customers that call competing service providers. For example, as a local exchange carrier, we do not use local service CPNI to track Customers that call local service competitors.

CPNI Approvals

(1) When Customer approval to use, disclose or permit access to Customer CPNI is required, we obtain approval through written methods. We honor a Customer's approval or disapproval until the Customer revokes or limits such approval or disapproval. We maintain all records of Customer approvals 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. Our notifications: (a) contain a statement that the Customer has a right, and we have a duty, under federal law, to protect the confidentiality of CPNI; (b) specify the types of information that constitute CPNI and the specific entities that will receive CPNI, describe the purposes for which the CPNI will be used, and inform the Customer of his or her right to disapprove those uses and deny or withdraw access to CPNI use at any time. With regard to the latter, we indicate that any approval, or disapproval, will remain in effect until the Customer affirmatively revokes or limits such approval or denial.
(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. However, we may provide a brief statement, in clear and neutral language, that describes the consequences directly resulting from the lack of access to CPNI. In addition, we may state that the Customer's consent to use his or her CPNI may enhance our ability to offer products and services tailored to meet the Customer's needs and that we will disclose the Customer's CPNI to any person upon the affirmative written request of the Customer.
(4) Our notifications are comprehensible and not misleading and, if written, are legible, sufficiently in large type, and placed in an area readily apparent to the Customer. And, if any portion of a notification is in another language, all portions of the notification will be in that language.
(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 wait at least 30 days after giving Customers notice and an opportunity to opt-out before assuming Customer approval to use, disclose, or permit access to CPNI and notify Customers of the applicable waiting period for a response before approval is assumed. For mail notifications, the 30 days begins to run on the third day following the date the notification was mailed.

(8) 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.

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 require valid photo ID or password for authentication on all In-office visits. We require a password for authentication on all customer initiated calls. Otherwise, we offer to contact the customer by calling the telephone number of record, send data to the address of record, or ask the customer to come into the office and provide valid photo ID.
(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. Any employee found violating the Company's CPNI Policies and Practices is subject to disciplinary action ranging from written warnings to termination, depending on the nature, frequency and severity of the violation(s).
(4) SCTC will notify any customer immediately of account changes including but not limited to password, customer response to company designed back-up means of authentication, on-line account, address of record, and any other record deemed required to notify customer. This notification will be through a voicemail or by USPS mail to the address of record as it was prior to the change.
New customers are exempt from this notification at service initiation.
(5) 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.
(6) 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.
(7) 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 and training 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.
(8) 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. That notice would be in the form of a letter and would include the Company's

name, a description of the opt-out mechanism(s) used, the problem(s) experienced, the remedy proposed and when it would be/was implemented, whether relevant state commission(s) were notified and what action was taken, a copy of any notice provided to customers, and contact information. We would submit the notice even if other methods by which consumers may opt-out were offered.

(9) Procedures to protect against Pretexting. Pretexting is the practice of pretending to be a particular customer or other authorized person in order to obtain access to that customer's call detail or other private communications record. The Company has employed the above procedures and safeguards in order to achieve reasonable measures designed to discover and protect against pretexting.

(10) SCTC policy requires this CPNI Policy Manual to be reviewed on an annual basis. This review is conducted at a time set by the General Manager each calendar year. The General Manager's annual review will include, but may not be limited to a review with it's consulting & legal firms and a review with the Board of Directors.

EMPLOYEE TRAINING CERTIFICATION - CPNI

On an annual basis an officer of our company must certify to the Federal Communications Commission (FCC) that it has established procedures that are adequate to ensure compliance with the FCC's Customer Proprietary Network Information (CPNI) rules.

One of the things that the officer is certifying to is that employees, especially those that have access to CPNI, have been trained on the CPNI rules. The training includes, but is not limited to, when employees are and are not authorized to use CPNI, and the authentication methods the company is using for both call detail and non-call detail information.

Our company's policy is to provide the training to all new employees when hired and then on an on-going annual basis, or more frequently, if needed.

By signing below, I acknowledge:

1) I have received the required training on the CPNI rules.

2) I have received the company's manual on CPNI Policies and Practices.

3) I understand the company's procedures for protecting CPNI.

4) I understand the company's disciplinary process if I use CPNI inappropriately. Any employee found violating the Company's CPNI Policies and Practices is subject to disciplinary action ranging from written warnings to termination, depending on the nature, frequency and severity of the violation(s).

5) I understand that if I have any questions at any time regarding the rules, I should immediately contact my immediate supervisor or a member of management.

Employee Printed Name: _____

Employee Signature: _____

Date: _____

_____ _____

Witnessed by the CPNI Compliance Officer Date