

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

Annual 64.2009(e) CPNI Certification for **2007**

Date filed: **February 28, 2008**

Name of company covered by this certification: **SST Long Distance Company, Inc.**

Form 499 Filer ID: **818176**

Name of signatory: Deborah K. Ailey

Title of signatory: Assistant Vice President

I, Deborah K. Ailey, certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the company has 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 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 (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 company **has 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  [electronic signature]

**SST Long Distance Company, Inc.**  
**Summary of CPNI Compliance Procedures**  
**February 28, 2008**

SST Long Distance Co., Inc. (“SST”) is in full compliance with the Commission’s rules governing use and disclosure of Customer Proprietary Network Information (“CPNI”), 47 C.F.R. §§ 64.2001 *et. seq.*

Training and Recordkeeping: SST management-level employees have reviewed the Commission’s revised CPNI rules, and the Commission’s associated Order, *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers’ Use of Customer Proprietary Network Information and Other Customer Information*, CC Docket No. 96-115, Report and Order and Further Notice of Proposed Rulemaking, FCC 07-22 (2007), and participated in several third-party training seminars on the topic. In addition, SST has purchased the CPNI compliance manual published by John Staurulakis, Inc. All SST employees were trained on the requirements of the new rules in November, 2007.

SST keeps a record of its own and its affiliates sales and marketing campaigns that use customer CPNI (including a description of the campaign, the specific CPNI that was used, and what products or services were offered), all disclosures of CPNI to third parties, and all instances where third parties were allowed access to CPNI, for a minimum of one year.

Outbound Market Review Process: SST has established a supervisory review process regarding its compliance with the Commission’s CPNI rules for outbound marketing situations and maintains records of this compliance for at least one year. Sales personnel must obtain supervisory approval of any proposed outbound marketing request for customer approval. Specifically, any outbound marketing campaigns require a detailed outline be submitted to the Business Office Manager for a CPNI Compliance Review. The outline will contain the following information.

- (1) The descriptive name of the marketing campaign.
- (2) The list of products and/or services to be offered in the campaign.
- (3) The listing of customers to be marketed and indicate whether all customers are to receive marketing or it is a selective marketing.
- (4) The listing of customers that will be excluded from the campaign because of their election to “Opt Out” of marketing campaigns.

After compliance review is completed, the Business Office Manager will denote acceptance or rejection of campaign on the outline submitted and enter same in CPNI Marketing Log.

Customer Consent: In its September, 2006 billing statements, SST sent all of its customers an up-to-date notice describing the FCC's rules, and the company's practices in safeguarding CPNI thereunder. In addition, each new customer is provided a similar notification of the company's practices in safeguarding CPNI and an Opt-Out consent form. In particular, this notice included the following information required by the Commission's rules, 47 C.F.R. § 64.2008(c):

- (1) The notice stated that the customer has a right, and the carrier has a duty, under federal law, to protect the confidentiality of CPNI;
- (2) The notice specified the types of information that constitute CPNI and the specific entities that will receive the CPNI, describe the purposes for which CPNI will be used, and inform the customer of his or her right to disapprove those uses, and deny or withdraw access to CPNI at any time;
- (3) The notice advised the customer of the precise steps the customer must take in order to grant or deny access to CPNI, and clearly stated that a denial of approval will not affect the provision of any services to which the customer subscribes;
- (4) The notice was comprehensible and was not misleading;
- (5) The notice was clearly legible, used sufficiently large type, and was placed in an area so as to be readily apparent to a customer;
- (6) No portion of the notice was translated into any language other than English;
- (7) The notice stated that the customer's approval to use CPNI may enhance SST's ability to offer products and services tailored to the customer's needs;
- (8) The notice did not include any statement attempting to encourage a customer to freeze third-party access to CPNI;
- (9) The notification stated that any denial of approval for the use of CPNI outside of the service to which the customer already subscribes from that carrier is valid until the customer affirmatively revokes or limits such denial; and
- (10) The opt-out consent form was provided together with the notice.

An "opt-out" consent form, which a customer could use to deny SST permission to use CPNI in marketing its services to him or her and share such CPNI with its affiliates, accompanied the notice. If a customer returns the form, SST adds a record of the customer's denial of permission to use CPNI to that customer's account records, and treats that election as permanent until changed. SST restricts its use of CPNI in marketing services to these customers to those services within the categories of services to which the customer already subscribes, as described in 47 C.F.R. § 64.2005.

SST does not use "opt-in" consent because it does not use independent contractors or joint venture partners in marketing its services.

Customer education and establishment of passwords: SST engaged in a substantial customer education campaign this past November and December to highlight the FCC's new CPNI rules in light of the concerns raised by "pretexting," and explain the introduction of passwords for customer accounts. These efforts consisted of the following steps:

- (1) SST placed a message in its customer's November, 2007 bills explaining what "pretexting" is and highlighting the FCC's new rules to protect against the dangers of this practice.
- (2) SST published a report of the new rules, entitled "SST Implements New FCC Rules to Safeguard Customer Records," in the December 2007 issue of its customer newsletter, the *SST Connection*.
- (3) SST added a spoken message delivered to customers calling SST while their calls were on hold, which explained that the Commission had enacted new, more protective rules to protect the privacy of account information, and encouraging customers to establish account passwords for added security. At the time they establish a password, customers are encouraged to establish a security question and answer to be used as a backup identification method in the event the customer forgets the password.
- (4) SST established a random password on all accounts where the customer had not otherwise selected a password. These passwords were not based on readily-available biographical information or account information, and were mailed to the customer's address of record, together with instructions on how to change the password, if desired. As of December 8, 2007, to gain access to the account, a customer calling SST is required to provide the password or correct response to the backup security question. If the customer cannot do so, the customer is offered the option of (a) having the SST representative call the customer at his telephone number of record; (b) having SST mail billing information to the customer's address of record; (c) visiting the SST office or a retail location and presenting valid photographic identification matching the customer's account information; (d) accessing the account online; or (e) establishing a new password after proper re-authentication.
- (5) SST sent a form to every business customer to request the names of authorized contacts. In addition, SST advised each business customer with procedures for establishing an account password and security questions. Residential customers were also given the option to identify authorized representatives, such as a spouse or other relative, who are permitted to discuss their account with SST personnel.
- (6) Customers who had established online access to their billing accounts were emailed by SST's billing agent and advised to re-establish account password and security questions. Customers who have established online access accounts must change their Passwords at least every 90 days.

SST provides notice by mail to the customer when the account password, the response to the back-up security question, or the customer's address of record, is created or changed.

Access to CPNI: Before SST representatives will discuss a customer's CPNI over the telephone, based on a customer-initiated contact, every customer must be authenticated through the use of the password established for the customer's account. If a customer calls SST but cannot provide the password established for his or her account, SST representatives will, at the customer's option: (a) call the customer back at the customer's telephone number of record; (b) send call detail information to the customer at the customer's address of record; or (c) assist customers with service and billing questions regarding specific billed call detail information, if the customer can provide such information without assistance from the SST service representative to support their on-phone request for assistance.

Customers seeking online access to their accounts must provide a password, which is not based on readily available biographical information, or account information, to do so. In addition, a customer may establish a security question and answer to be used as a backup authentication method in the event the customer forgets the password. Account passwords must be changed every 90 days.

A customers seeking access to CPNI in an SST retail store must present valid photographic identification matching the customer's account information.

Breaches of Security: A breach of a customer's CPNI occurs when a person, without authorization or exceeding authorization, has intentionally gained access to, used, or disclosed CPNI. If a breach of a customer's CPNI occurs, then SST will notice the United States Secret Service ("USSS") and the Federal Bureau of Investigation ("FBI") through a central reporting facility, as soon as practicable, but no later than seven days after it makes a reasonable determination that the breach has occurred.

Notwithstanding any state or local law to the contrary, SST will not notify customers or disclose the breach to the public until seven full business days have passed after SST's notification to the USSS and FBI, except in cases where SST believes that there is an extraordinarily urgent need to notify any class of affected customers more quickly, in order to avoid immediate and irreparable harm. In such cases, SST will so indicate in its notifications to the USSS and FBI, and consult with the relevant investigating agency before notifying customers. SST will cooperate with the relevant investigating agency's request to minimize any adverse effects of such customer notification.

If the relevant investigating agency makes a reasonable determination that public disclosure of the breach would impede or compromise an ongoing or potential criminal investigation or national security, and directs SST to delay disclosure of the breach to customer or to the public, SST will comply with that directive.

SST will keep a record of any breaches discovered, notifications made to the USSS and FBI, and notifications to customers, including the dates of discovery and notification, a detailed description of the CPNI that was the subject of the breach, and the circumstances of the breach, for at least two years.