

§ 64.2009

CPNI, as long as the carrier clearly communicates that the customer can deny access to his CPNI for the call.

[67 FR 59212, Sept. 20, 2002]

EFFECTIVE DATE NOTE: At 67 FR 59212, Sept. 20, 2002, §64.2008 was added. This section contains information collection requirements and will not become effective until approval has been given by the Office of Management and Budget.

§ 64.2009 Safeguards required for use of customer proprietary network information.

(a) Telecommunications carriers must implement a system by which the status of a customer's CPNI approval can be clearly established prior to the use of CPNI.

(b) Telecommunications carriers must train their personnel as to when they are and are not authorized to use CPNI, and carriers must have an express disciplinary process in place.

(c) All carriers shall maintain a record, electronically or in some other manner, of their own and their affiliates' sales and marketing campaigns that use their customers' CPNI. All carriers shall maintain a record of all instances where CPNI was disclosed or provided to third parties, or where third parties were allowed access to CPNI. The record must include a description of each campaign, the specific CPNI that was used in the campaign, and what products and services were offered as a part of the campaign. Carriers shall retain the record for a minimum of one year.

(d) Telecommunications carriers must establish a supervisory review process regarding carrier compliance with the rules in this subpart for outbound marketing situations and maintain records of carrier compliance for a minimum period of one year. Specifically, sales personnel must obtain supervisory approval of any proposed outbound marketing request for customer approval.

(e) A telecommunications carrier must have an officer, as an agent of the carrier, sign a compliance certificate on an annual basis stating that the officer has personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the rules in this sub-

47 CFR Ch. I (10-1-03 Edition)

part. The carrier must provide a statement accompanying the certificate explaining how its operating procedures ensure that it is or is not in compliance with the rules in this subpart.

(f) Carriers must provide written notice within five business days to the Commission 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.

(1) The notice shall be in the form of a letter, and shall include the carrier's name, a description of the opt-out mechanism(s) used, the problem(s) experienced, the remedy proposed and when it will be/was implemented, whether the relevant state commission(s) has been notified and whether it has taken any action, a copy of the notice provided to customers, and contact information.

(2) Such notice must be submitted even if the carrier offers other methods by which consumers may opt-out.

[63 FR 20338, Apr. 24, 1998, as amended at 64 FR 53264, Oct. 1, 1999; 67 FR 59213, Sept. 20, 2002]

EFFECTIVE DATE NOTE: At 67 FR 59213, Sept. 20, 2002, §64.2009 was amended by revising paragraphs (c) and (d) and by adding paragraph (f). These paragraphs contain information collection requirements and will not become effective until approval has been given by the Office of Management and Budget.

Subpart V—Telecommunications Carrier Systems Security and Integrity Pursuant to the Communications Assistance for Law Enforcement Act (CALEA)

SOURCE: 64 FR 51469, Sept. 23, 1999, unless otherwise noted.

§ 64.2100 Purpose.

Pursuant to the Communications Assistance for Law Enforcement Act, Public Law 103-414, 108 Stat. 4279 (1994) (codified as amended in sections of 18 U.S.C. and 47 U.S.C.), this subpart contains rules that require a telecommunications carrier to ensure that any interception of communications or access to call-identifying information effected within its switching premises can be activated only in accordance