

Appendix B**Final Rules**

Subpart U of Part 64, of Title 47 of the Code of Federal Regulations is amended to read as follows:

SUBPART U – CUSTOMER PROPRIETARY NETWORK INFORMATION

1. Section 64.2003(k) is amended to read as follows:
 - (k) *Telecommunications carrier or carrier.* The terms “telecommunications carrier” or “carrier” shall have the same meaning as set forth in section 3(44) of the Communications Act of 1934, as amended, 47 U.S.C. 153(44). For the purposes of this Subpart, the term “telecommunications carrier” or “carrier” shall include “interconnected VoIP provider” as that term is defined in section 9.3 of these rules.
2. Section 64.2003 is amended by redesignating paragraphs (a)-(l) and by adding the following paragraphs:
 - (a) *Account information.* “Account information” is information that is specifically connected to the customer’s service relationship with the carrier, including such things as an account number or any component thereof, the telephone number associated with the account, or the bill’s amount.
 - (b) *Address of record.* An “address of record,” whether postal or electronic, is an address that the carrier has associated with the customer’s account for at least 30 days.
 - (d) *Call detail information.* Any information that pertains to the transmission of specific telephone calls, including, for outbound calls, the number called, and the time, location, or duration of any call and, for inbound calls, the number from which the call was placed, and the time, location, or duration of any call.
 - (l) *Readily available biographical information.* “Readily available biographical information” is information drawn from the customer’s life history and includes such things as the customer’s social security number, or the last four digits of that number; mother’s maiden name; home address; or date of birth.
 - (p) *Telephone number of record.* The telephone number associated with the underlying service, not the telephone number supplied as a customer’s “contact information.”
 - (q) *Valid photo ID.* A “valid photo ID” is a government-issued means of personal identification with a photograph such as a driver’s license, passport, or comparable ID that is not expired.
3. Section 64.2005(c)(3) is amended to read as follows:
 - (3) LECs, CMRS providers, and interconnected VoIP providers may use CPNI, without customer approval, to market services formerly known as adjunct-to-basic services, such as, but not limited to, speed dialing, computer-provided directory assistance, call monitoring, call tracing, call blocking, call return, repeat dialing, call tracking, call waiting, caller I.D., call forwarding, and certain centrex features.

4. Section 64.2007 is amended by deleting paragraphs (b)(2) and (b)(3), and revising paragraph (b)(1) to read as follows:
 - (b) *Use of Opt-Out and Opt-In Approval Processes.* A telecommunications carrier may, subject to opt-out approval or opt-in approval, use its customer's individually identifiable CPNI for the purpose of marketing communications-related services to that customer. A telecommunications carrier may, subject to opt-out approval or opt-in approval, disclose its customer's individually identifiable CPNI, for the purpose of marketing communications-related services to that customer, to its agents and its affiliates that provide communications-related services. A telecommunications carrier may also permit such persons or entities to obtain access to such CPNI for such purposes. Except for use and disclosure of CPNI that is permitted without customer approval under section § 64.2005, or that is described in this paragraph, or as otherwise provided in section 222 of the Communications Act of 1934, as amended, a telecommunications carrier may only use, disclose, or permit access to its customer's individually identifiable CPNI subject to opt-in approval.
5. Section 64.2009 is amended by revising paragraph (e) to read as follows:
 - (e) A telecommunications carrier must have an officer, as an agent of the carrier, sign and file with the Commission a compliance certificate on an annual basis. The officer must state in the certification that he or she has personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the rules in this subpart. 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. In addition, the carrier must include an explanation of any actions taken against data brokers and a summary of all customer complaints received in the past year concerning the unauthorized release of CPNI. This filing must be made annually with the Enforcement Bureau on or before March 1 in EB Docket No. 06-36, for data pertaining to the previous calendar year.
6. Section 64.2010 is added to read as follows:

§ 64.2010 Safeguards on the disclosure of customer proprietary network information

- (a) *Safeguarding CPNI.* Telecommunications carriers must take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI. Telecommunications carriers must properly authenticate a customer prior to disclosing CPNI based on customer-initiated telephone contact, online account access, or an in-store visit.
- (b) *Telephone access to CPNI.* Telecommunications carriers may only disclose call detail information over the telephone, based on customer-initiated telephone contact, if the customer first provides the carrier with a password, as described in paragraph (e) of this section, that is not prompted by the carrier asking for readily available biographical information, or account information. If the customer does not provide a password, the telecommunications carrier may only disclose call detail information by sending it to the customer's address of record, or, by calling the customer at the telephone number of record. If the customer is able to provide call detail information to the telecommunications carrier during a customer-initiated call without the telecommunications carrier's assistance, then the telecommunications carrier is permitted to discuss the call detail information provided by the customer.
- (c) *Online access to CPNI.* A telecommunications carrier must authenticate a customer without the use of readily available biographical information, or account information, prior to

allowing the customer online access to CPNI related to a telecommunications service account. Once authenticated, the customer may only obtain online access to CPNI related to a telecommunications service account through a password, as described in paragraph (e) of this section, that is not prompted by the carrier asking for readily available biographical information, or account information.

- (d) *In-store access to CPNI.* A telecommunications carrier may disclose CPNI to a customer who, at a carrier's retail location, first presents to the telecommunications carrier or its agent a valid photo ID matching the customer's account information.
- (e) *Establishment of a Password and Back-up Authentication Methods for Lost or Forgotten Passwords.* To establish a password, a telecommunications carrier must authenticate the customer without the use of readily available biographical information, or account information. Telecommunications carriers may create a back-up customer authentication method in the event of a lost or forgotten password, but such back-up customer authentication method may not prompt the customer for readily available biographical information, or account information. If a customer cannot provide the correct password or the correct response for the back-up customer authentication method, the customer must establish a new password as described in this paragraph.
- (f) *Notification of account changes.* Telecommunications carriers must notify customers immediately whenever a password, customer response to a back-up means of authentication for lost or forgotten passwords, online account, or address of record is created or changed. This notification is not required when the customer initiates service, including the selection of a password at service initiation. This notification may be through a carrier-originated voicemail or text message to the telephone number of record, or by mail to the address of record, and must not reveal the changed information or be sent to the new account information.
- (g) *Business Customer Exemption.* Telecommunications carriers may bind themselves contractually to authentication regimes other than those described in this section for services they provide to their business customers that have both a dedicated account representative and a contract that specifically addresses the carriers' protection of CPNI.

7. Section 64.2011 is added to read as follows:

§ 64.2011 Notification of customer proprietary network information security breaches

- (a) A telecommunications carrier shall notify law enforcement of a breach of its customers' CPNI as provided in this section. The carrier shall not notify its customers or disclose the breach publicly, whether voluntarily or under state or local law or these rules, until it has completed the process of notifying law enforcement pursuant to paragraph (b).
- (b) As soon as practicable, and in no event later than seven (7) business days, after reasonable determination of the breach, the telecommunications carrier shall electronically notify the United States Secret Service (USSS) and the Federal Bureau of Investigation (FBI) through a central reporting facility. The Commission will maintain a link to the reporting facility at <http://www.fcc.gov/eb/cpni>.
 - (1) Notwithstanding any state law to the contrary, the carrier shall not notify customers or disclose the breach to the public until 7 full business days have passed after notification to the USSS and the FBI except as provided in paragraphs (2) and (3).

-
- (2) If the carrier believes that there is an extraordinarily urgent need to notify any class of affected customers sooner than otherwise allowed under paragraph (1), in order to avoid immediate and irreparable harm, it shall so indicate in its notification and may proceed to immediately notify its affected customers only after consultation with the relevant investigating agency. The carrier shall cooperate with the relevant investigating agency's request to minimize any adverse effects of such customer notification.
- (3) If the relevant investigating agency determines that public disclosure or notice to customers would impede or compromise an ongoing or potential criminal investigation or national security, such agency may direct the carrier not to so disclose or notify for an initial period of up to 30 days. Such period may be extended by the agency as reasonably necessary in the judgment of the agency. If such direction is given, the agency shall notify the carrier when it appears that public disclosure or notice to affected customers will no longer impede or compromise a criminal investigation or national security. The agency shall provide in writing its initial direction to the carrier, any subsequent extension, and any notification that notice will no longer impede or compromise a criminal investigation or national security and such writings shall be contemporaneously logged on the same reporting facility that contains records of notifications filed by carriers.
- (c) *Recordkeeping.* All carriers shall maintain a record, electronically or in some other manner, of any breaches discovered, notifications made to the USSS and the FBI pursuant to paragraph (b), and notifications made to customers. The record must include, if available, dates of discovery and notification, a detailed description of the CPNI that was the subject of the breach, and the circumstances of the breach. Carriers shall retain the record for a minimum of 2 years.
- (d) *Definitions.* As used in this section, a "breach" has occurred when a person, without authorization or exceeding authorization, has intentionally gained access to, used, or disclosed CPNI.
- (e) This section does not supersede any statute, regulation, order, or interpretation in any State, except to the extent that such statute, regulation, order, or interpretation is inconsistent with the provisions of this section, and then only to the extent of the inconsistency.