Customer Proprietary Network Information

Customer proprietary network information (CPNI) means information that relates to the quantity, technical configuration, type, destination, location, and amount of use of our service by you and information regarding your use of our service contained in documentation we submit to the Telecommunications Relay Service Fund (TRS) administrator in connection with a request for compensation for the provision of TRS.

FCC regulations allow us to use, disclose, or permit access to CPNI for the purpose of providing or lawfully marketing service offerings among the categories of service (*i.e.*, type of TRS) for which we are currently your default provider as defined by FCC regulations without your approval. Where we provide different categories of TRS, and are currently the default provider for you for more than one category of TRS, we may share CPNI among any of our affiliated entities that provide a TRS offering to you.

Where we provide different categories of TRS, but are currently not the default provider for you for more than one TRS offering, we may not share CPNI with our affiliates, except as provided in FCC Rule §64.5107(b). We may not use, disclose, or permit access to CPNI except as described below.

We may not use, disclose, or permit access to CPNI to market to a customer TRS offerings that are within a category of TRS for which we are not currently your default provider, unless you give us approval to do so.

We may not identify or track your CPNI when you call competing TRS providers and, we may not use, disclose or permit access to CPNI related to your calls processed through a competing TRS provider.

We may use, disclose, or permit access to CPNI, without your approval, in the following circumstances, if applicable:

(1) We may use, disclose or permit access to CPNI derived from our provision of TRS without your approval, for the provision of CPE or iTRS access technology, and call answering, voice or video mail or messaging, voice or video storage and retrieval services.

(2) We may use, disclose, or permit access to CPNI, without your approval, in the provision of inside wiring installation, maintenance, and repair services.

(3) We may use CPNI, without your approval, to market services formerly known as adjunct-to-basic services, such as, but not limited to, speed dialing, call waiting, caller I.D., and call forwarding, only to you if you are currently registered with us as your TRS default provider.

(4) We must use, disclose, or permit access to your CPNI to the extent necessary to:

(i) Accept and handle 911/E911 calls;

(ii) Access, either directly or via a third party, a commercially available database that will

allow us to determine an appropriate Public Safety Answering Point, designated statewide default answering point, or appropriate local emergency authority that corresponds to the caller's location;
(iii) Relay the 911/E911 call to that entity; and
(iv) Facilitate the dispatch and response of emergency service or law enforcement personnel to the caller's location, in the event that the 911/E911 call is disconnected or the caller becomes incapacitated.

(5) We must use, disclose, or permit access to CPNI upon request by the administrator of the TRS Fund, as that term is defined in FCC Rule §64.604(c), or by the FCC for the purpose of administration and oversight of the TRS Fund, including the investigation and prevention of fraud, abuse, and misuse of TRS and seeking repayment to the TRS Fund for non-compensable minutes.

(6) We may use, disclose, or permit access to your CPNI to protect our rights or property, or to protect users of our services, other TRS providers, and the TRS Fund from fraudulent, abusive, or unlawful use of such services.

We may ask for your approval to use your CPNI through written, oral, electronic, or sign language methods. Your approval or disapproval for us to use, disclose, or permit access to your CPNI will remain in effect until you revokes or limit such approval or disapproval. We will accept any such customer revocation, whether in written, oral, electronic, or sign language methods.
We must maintain records of approval, whether oral, written, electronic, or sign language, during the time period that the approval or disapproval is in effect and for at least one year thereafter. We may seek your approval for us of CPNI either through Opt-in or Opt-out procedures. Opt-in approval requires that we obtain from you affirmative, express consent allowing the requested CPNI usage, disclosure, or access after you are provided appropriate notification of our request consistent with the FCC requirements. With opt-out approval, you are deemed to have consented to the use, disclosure, or access to your CPNI if you fail to object within the waiting period discussed below after we provide to you appropriate notification of our request for consent set forth below.

We may only use, disclose, or permit access to your CPNI with the opt-in approval, except as follows:
(i) Where we are permitted to use, disclose, or permit access to CPNI without your approval.
(ii) Where we are permitted to use, disclose, or permit access to CPNI by making use of customer opt-in or opt-out approval as discussed herein.

We may make use of customer opt-in or opt-out approval to take the following actions with respect to CPNI:
(i) Use your CPNI for the purpose of lawfully marketing to you TRS-related services.
(ii) Disclose your CPNI to our agents and its affiliates that provide TRS-related services for the purpose of lawfully marketing to you TRS-related services. We may also permit such persons or entities to obtain access to your CPNI for such purposes.

Customer Proprietary Network Information

Prior to requesting your approval to use, disclose, or permit access to your CPNI, we will notify you of your right to deny or restrict use of, disclosure of, and access to your CPNI.

We will maintain records of notification, whether oral, written, electronic, or sign language, during the time that your approval is in effect and for at least one year thereafter. We will provide individual notice to you when soliciting approval to use, disclose, or permit access to your CPNI.

The notification will provide sufficient information in clear and unambiguous language to enable you to make an informed decision as to whether to permit us to use, disclose, or permit access to your CPNI.

The notification will state that you have a right to deny us the right to use, disclose or permit access to your CPNI, and we have a duty, under federal law, to honor your right and to protect the confidentiality of CPNI. The notification will specify the types of information that constitute CPNI and the specific entities that will use, receive or have access to the CPNI, describe the purposes for which CPNI will be used, and inform you of your right to disapprove those uses, and deny or withdraw your consent to use, disclose, or permit access to access to CPNI at any time.

The notification will advise you of the precise steps you must take to grant or deny use, disclosure, or access to CPNI, and will clearly state that your denial of approval will not affect our provision of any services to you. However, we may provide a brief statement, in clear and neutral language, describing consequences directly resulting from the lack of access to CPNI. We will provide the notification in a manner that is accessible to you, comprehensible, and not misleading. If we provide written notification to you, the notice will be clearly legible, use sufficiently large type, and be placed in an area so as to be readily apparent to you. If any portion of a notification is translated into another language, then all portions of the notification will be translated into that language.

We may state in the notification that your approval to use CPNI may enhance our ability to offer products and services tailored to your needs. We also may state in the notification that we may be compelled to disclose CPNI to any person upon affirmative written request by you. The notification will state that any approval or denial of approval for the use of CPNI outside of the service for which we are the default provider for you is valid until you affirmatively revoke or limit such approval or denial. Our solicitation for approval to use, disclose, or have access to your CPNI must be proximate to the notification of your CPNI rights to non-disclosure.

We will wait a 30-day minimum period after giving you notice and an opportunity to opt-out before assuming your approval to use, disclose, or permit access to CPNI. We may, in our discretion, provide for a longer period. We will notify you as to the applicable waiting period for a response before approval is assumed. In the case of an electronic form of notification, the waiting period will begin to run from the date on which the notification is sent; and in the case of notification by mail, the waiting period shall begin to run on the third day following the date that the notification is mailed. If we use the opt-out mechanism, we will provide notices to you every two years.

If we use email to provide opt-out notices, we will comply with the following requirements in addition to the requirements generally applicable to notification:

(i) We will obtain express, verifiable, prior approval from you to send notices via email regarding our service in general, or CPNI in particular;

(ii) We will either:

(A) Allow you to reply directly to the email containing the CPNI notice in order to opt-out; or

(B) Include within the email containing the CPNI notice a conspicuous link to a Web page that provides to you a readily usable opt-out mechanism;

(iii) Opt-out email notices that are returned to us as undeliverable will be sent to you in another form before we may consider you to have received notice;

(iv) When we use email to send CPNI notices to you we will ensure that the subject line of the message clearly and accurately identifies the subject matter of the email; and

(v) We will make available to you a method to opt-out that is of no additional cost to you and that is available 24 hours a day, seven days a week. We may satisfy this requirement through a combination of methods, so long as you have the ability to opt-out at no cost and are able to effectuate that choice whenever you choose.

We may provide notification to obtain opt-in approval through oral, sign language, written, or electronic methods. The contents of any such notification will comply with the requirements set forth herein.

We may use oral, text, or sign language notice to obtain limited, one-time use of CPNI for inbound and outbound customer telephone, TRS, or point-to-point contacts for the duration of the call, regardless of whether we use opt-out or opt-in approval based on the nature of the contact. The contents of any such notification shall comply with the requirements set forth herein, except that we may omit any of the following notice provisions if not relevant to the limited use for which we seek CPNI:

(i) We need not advise you that if you have opted-out previously, no action is needed to maintain the opt-out election;

(ii) We need not advise you that we may share CPNI with our affiliates or third parties and need not name those entities, if the limited CPNI usage will not result in use by, or disclosure to, an affiliate or third party;

(iii) We need not disclose the means by which you can deny or withdraw future access to CPNI, so long as we explain to you that the scope of the approval we seek is limited to one-time use; and

(iv) We may omit disclosure of the precise steps you must take to grant or deny access to CPNI, as long as we clearly communicates that you can deny access to your CPNI for the call.

Policies Customer Proprietary Network Information.

Safeguards required for use of customer proprietary network information.

Customer Proprietary Network Information

(a) Pursuant to FCC regulations, we must implement a system by which the status of a customer's CPNI approval can be clearly established prior to the use of CPNI. We require all personnel, including any agents, contractors, and subcontractors, who have contact with customers to verify the status of a customer's CPNI approval before using, disclosing, or permitting access to the customer's CPNI.
(b) We must train all personnel, including any agents, contractors, and subcontractors, as to when they are and are not authorized to use CPNI, including procedures for verification of the status of a customer's CPNI approval. We must have an express disciplinary process in place, including in the case of agents, contractors, and subcontractors, a right to cancel the applicable contract(s) or otherwise take disciplinary action.
(c) We shall maintain a record, electronically or in some other manner, of our own and our affiliates' sales and marketing campaigns that use customers' CPNI. We must maintain a record of all instances where CPNI is disclosed or provided to third parties, or where third parties are allowed access to CPNI. The record shall include a description of each campaign, the specific CPNI that was used in the campaign, including the customer's name, and what products and services were offered as a part of the campaign. We shall retain the record for a minimum of three years.
(d) We have establish a supervisory review process regarding our compliance with the FCC's CPNI rules for outbound marketing situations and maintain records of our compliance for a minimum period of three years. Sales personnel must obtain supervisory approval in writing of any proposed outbound marketing request for customer approval. Such approval must come from the CEO and the Compliance Director.
(e) The CEO and Compliance Director shall sign and file with the FCC a compliance certification on an annual basis. The signatories shall state in the certification that he or they have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the FCC's rules. We will provide a statement accompanying the certification explaining how our operating procedures ensure that we are in compliance with the rules. In addition, we will include an explanation of any actions taken against data brokers, a summary of all customer complaints received in the past year concerning the unauthorized release of CPNI, and a report detailing all instances where we, or our agents, contractors, or subcontractors, used, disclosed, or permitted access to CPNI without complying with the procedures specified in the FCC's rules. This filing shall be included in the annual report filed with the FCC pursuant to FCC Rule §64.606(g) for data pertaining to the previous year.
(f) We shall provide written notice within five business days to the Disability Rights Office of the Consumer and Governmental Affairs Bureau of 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.

(1) The notice shall be in the form of a letter, and shall include our 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, if applicable, and whether the state commission(s) has taken any action, a copy of the notice provided to customers, and contact information.
(2) Such notice shall be submitted even if the we offer other methods by which consumers may opt-out.

Customer Proprietary Network Information

Safeguarding CPNI data.

(a) *Safeguarding CPNI.* InnoCaption is required to take all reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI. We must authenticate a customer prior to disclosing CPNI based on a customer-initiated telephone contact, TRS call, point-to-point call, online account access, or an in-store visit.
(b) *Telephone, TRS, and point-to-point access to CPNI.* We must authenticate a customer without the use of readily available biographical information, or account information, prior to allowing the customer telephonic, TRS, or point-to-point access to CPNI related to his or her TRS account. Alternatively, the customer may obtain telephonic, TRS, or point-to-point access to CPNI related to his or her TRS account through a password, as described in paragraph (e) of this section.
(c) *Online access to CPNI.* We 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 his or her TRS account. Once authenticated, the customer may only obtain online access to CPNI related to his or her TRS account through a password, as described in paragraph (e) of this section.
(d) *In-store access to CPNI.* We may disclose CPNI to a customer who, at our retail location, first presents to the TRS provider 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, we must authenticate the customer without the use of readily available biographical information, or account information. We 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 backup customer authentication method, the customer shall establish a new password as described in this paragraph.
(f) *Notification of account changes.* We 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 voicemail, text message, or video mail to the telephone number of record, by mail to the physical address of record, or by email to the email address of record, and shall not reveal the changed information or be sent to the new account information.

Notification of customer proprietary network information security breaches.

(a) We must notify law enforcement of a breach of customers' CPNI as provided in this section. We may not notify our customers or disclose the breach publicly, whether voluntarily or under state or local law, until we have completed the process of notifying law enforcement pursuant to paragraph (b) of this section. We must file a copy of the notification with the Disability Rights Office of the Consumer and Governmental Affairs Bureau of the FCC at the same time as when we notify our customers.

(b) As soon as practicable, and in no event later than seven (7) business days, after reasonable determination of the breach, we must electronically notify the United States Secret Service (USSS) and the Federal Bureau of Investigation (FBI) through a central reporting facility. The FCC maintains a link to the reporting facility at *http://www.fcc.gov/eb/cpni.*

(1) Notwithstanding any state law to the contrary, FCC rules prohibit us from notifying customers or disclosing the breach to the public until seven full business days have passed after notification to the USSS and the FBI except as provided in paragraphs (b)(2) and (3) of this section.

(2) If we believe there is an extraordinarily urgent need to notify any class of affected customers sooner than otherwise allowed under paragraph (b)(1) of this section, in order to avoid immediate and irreparable harm, we must so indicate in our notification and may proceed to immediately notify our affected customers only after consultation with the relevant investigating agency. We must 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 us 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 us 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 us, 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 us.

(c) *Customer notification.* After we have completed the process of notifying law enforcement pursuant to paragraph (b) of this section, and consistent with the waiting requirements specified in paragraph (b) of this section, we will notify our customers of a breach of those customers' CPNI.

(d) *Recordkeeping.* We will 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) of this section, 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. We will retain the record for a minimum of 2 years.

(e) *Definition.* 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.

(f) We will comply with any state statute, regulation, order, or interpretation, except to the extent that such state, regulation, order, or interpretation is inconsistent with the provisions of this section, and then only to the extent of the inconsistency.