

**CPNI POLICY ACKNOWLEDGMENT FORM**

I hereby state and acknowledge that I have either received a copy or have access to a copy of the CUSTOMER PROPRIETARY NETWORK INFORMATION COMPLIANCE MANUAL, that I am responsible for reviewing and understanding this Manual, and that I understand that any violation of the Company's CPNI procedures may result in disciplinary action.

\_\_\_\_\_  
Signature

\_\_\_\_\_  
Date

\_\_\_\_\_  
Print name

WITNESSED:

CPNI COMPLIANCE OFFICER

\_\_\_\_\_  
Signature

\_\_\_\_\_  
Date

\_\_\_\_\_  
Print name

# **CUSTOMER PROPRIETARY NETWORK INFORMATION (CPNI) COMPLIANCE MANUAL**

This Manual governs all use of customer proprietary network information (CPNI) by all Company employees, agents, independent contractors and joint venture partners.

**It is the official policy of the Company that all access, use, disclosure or distribution of CPNI be in accordance with the customer privacy safeguards set forth in the Communications Act (47 U.S.C. §222) and the Federal Communications Commission (FCC) Rules (47 C.F.R. §§64.2001 through 64.2011), and that all Company employees, agents, independent contractors and joint venture partners who handle the Company's CPNI are aware of these customer privacy safeguards and comply fully with them. IT IS THE OFFICIAL POLICY OF THIS COMPANY THAT CPNI IS NOT TO BE DISCLOSED TO ANYONE, EXCEPT AS SPECIFICALLY AUTHORIZED IN THIS MANUAL, UNDER PENALTY OF POSSIBLE EMPLOYMENT TERMINATION.**

It is the responsibility of all Company employees, agents, independent contractors and joint venture partners to read and review this Manual, and to seek clarification from the Company's CPNI Compliance Officer regarding any CPNI-related questions, before accessing, using, disclosing or distributing CPNI in any manner and for any purpose. It is further the responsibility of every Company employee, agent, independent contractor and joint venture partner to comply fully with all federal CPNI requirements, and to seek clarification from the Company's CPNI Compliance Officer any time that an access, use, disclosure or distribution of CPNI appears to be questionable.

The FCC's rules place stringent restrictions upon CPNI access, use, disclosure and distribution to "independent contractors" for marketing purposes. **IT IS THE OFFICIAL POLICY OF THIS COMPANY THAT CPNI WILL NOT BE USED IN MARKETING CAMPAIGNS.**

**VoIP Services:** The FCC's CPNI Rules (47 C.F.R. §§64.2001 through 64.2011) apply to all providers of telecommunications services and to all providers of interconnected Voice over Internet Protocol ("VoIP") services.

## **I. Customer Proprietary Network Information ("CPNI")**

CPNI is defined in Section 222(h) of the Communications Act as (A) information that relates to the quantity, technical configuration, type, destination, and amount of use of a telecommunications service subscribed to by any customer of a wireline or wireless telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and (B) information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier (except that CPNI does not include subscriber list information).

Generally, CPNI includes personal information regarding a consumer's use of his or her wireline and/or wireless telecommunications services. CPNI encompasses information such as: (a) the telephone numbers called by a customer; (b) the telephone numbers from which a customer receives calls; (c) the frequency, duration, timing and location of a customer's phone calls, and (d) the telecommunications and information services purchased by a customer (including, but not limited to, local exchange, toll, cellular, PCS, paging, data transmission, call waiting, call

forwarding, call blocking, PIC freeze, three-way calling, conference calling, voice mail, Internet access, call back, caller identification, call trace and toll denial services).

**Call detail information** (also known as “call records”) is a category of CPNI that the FCC has determined to be particularly sensitive from a privacy standpoint and that may be sought by pretexters, hackers and other unauthorized entities for illegitimate purposes. Call detail information includes any information that pertains to the transmission of a specific telephone call to or from a specific customer, including: (a) the number called (for outbound calls); (b) the number from which the call was placed (for inbound calls); and (c) the date, time, location and/or duration of the call (for all calls). The FCC has imposed additional restrictions upon the release of call detail information over the telephone unless the requesting party can clearly authenticate himself or herself as the customer to whom the call detail information applies.

Information regarding **customer preferred carrier (“PC”) freezes** (including preferred interexchange carrier (“PIC”) freezes) constitutes CPNI. However, the FCC has determined that PC freeze information is less sensitive than other CPNI, and has granted limited forbearance so that it can be exchanged with other carriers without advance customer notice and consent.

**Subscriber list information** (that is, subscriber names, addresses, phone numbers and/or advertising classifications that a carrier or its affiliate have published, or provided for publication, in a telephone directory) is **not** CPNI because it is deemed to be more like aggregate customer information than personal, individually identifiable customer information. Subscriber list information may be used by a carrier (or disclosed to its agents, independent contractors, affiliates and/or third parties) to publish telephone directories without the approval of the “listed” subscribers (that is, those subscribers that do not have unlisted telephone numbers). Subscriber list information must be provided by carriers to third parties for the purpose of publishing directories, and must be so provided on a timely and unbundled basis at reasonable and nondiscriminatory rates, terms and conditions. **NOTE:** Unlisted phone numbers are not included in subscriber list information, and may not be used by a carrier, or disclosed to its affiliates or third parties, for the purpose of publishing telephone directories.

**Subscriber list information (PLUS unlisted subscriber names, addresses and phone numbers)** must be provided to emergency services and emergency support services for the purposes of delivering (and/or assisting in the delivery of) emergency services. This information must be provided on a timely and unbundled basis at reasonable and nondiscriminatory rates, terms and conditions.

**NOTE:** “Subscriber list information” contains only publicly available information that has been, or will soon be, published in one or more directories, whereas **“billing name and address information”** (“BNA”) may include information for unlisted as well as listed numbers. The FCC’s rules restrict the release of BNA to certain specific circumstances.

## II. Use and Disclosure of CPNI Is Restricted

**GENERAL RULE:** Because CPNI includes information that is personal and individually identifiable, privacy concerns have led Congress and the FCC to impose restrictions upon its use and disclosure, and upon the provision of access to it by individuals or entities inside and outside the Company.

In the wake of the improper provision or sale of CPNI to certain Internet sites, the FCC has made it clear that it will impose swift and potentially severe sanctions upon companies that violate

its CPNI requirements. The FCC has stated that it expects carriers to take **“every reasonable precaution”** to protect the confidentiality of proprietary and personal customer information. The FCC has put carriers on notice that it will infer from evidence that a pretexter obtained access to a customer’s CPNI that the carrier did not sufficiently protect that customer’s CPNI. The carrier will then have the **burden of demonstrating** to the FCC that it took reasonable steps to protect CPNI from unauthorized disclosure (in light of the threat posed by pretexting and the sensitivity of the customer information at issue) if it is to escape forfeitures or other sanctions.

### **III. CPNI Compliance Officer**

The Company has designated a CPNI Compliance Officer who is responsible for: (1) communicating with the Company’s attorneys and/or consultants regarding CPNI responsibilities, requirements and restrictions; (2) supervising the training of Company employees and agents who use or have access to CPNI; (3) supervising the use, disclosure, distribution or access to the Company’s CPNI by independent contractors and joint venture partners; (4) maintaining records regarding the use of CPNI in marketing campaigns; and (5) receiving, reviewing and resolving questions or issues regarding use, disclosure, distribution or provision of access to CPNI.

The Company’s current CPNI Compliance Officer is \_\_\_\_\_.

In addition to the specific matters required to be reviewed and approved by the Company’s CPNI Compliance Officer, Company employees, agents, independent contractors and joint venture partners are strongly encouraged to bring any and all other questions, issues or uncertainties regarding the use, disclosure, or access to CPNI to the attention of the Company’s CPNI Compliance Officer for appropriate investigation, review and guidance. The extent to which a particular employee or agent brought a CPNI matter to the attention of the CPNI Compliance Officer and complied with the CPNI Compliance Officer’s instructions or guidance constitutes a material consideration in any disciplinary action brought against the employee or agent for impermissible use, disclosure, distribution or access to CPNI.

### **IV. Training and Contract Arrangements Regarding CPNI**

#### **A. Employee and Agent Training**

Various Company employees and agents may access, use, disclose or distribute customer records containing CPNI. These employees and agents may include: (a) officers and managers; (b) customer service representatives; (c) dispute resolution personnel; (d) accountants and bookkeepers; (e) billing and collection personnel; (f) sales and marketing representatives; (g) account representatives; and (h) technicians and installers.

Before accessing, using, disclosing or distributing any customer’s CPNI, a Company employee or agent must complete the following CPNI Training Program:

1. The employee or agent must receive, read and review this Manual, including the attached copies of (a) the Company’s CPNI notices (Attachments 1,2 and 3); (b) the Company’s Customer CPNI Request Form (Attachment 4); and (c) the template for the Company’s annual CPNI Compliance Certificate (Attachment 5).
2. The employee or agent must attend a group training session (or, where timing and/or other circumstances render a group training session impracticable, a private meeting) with the

Company's CPNI Compliance Officer during which this Manual will be reviewed and discussed.

3. Employees and agents must attend annual Company reviews of CPNI policies, requirements and issues.

## **B. Contract Arrangements for Agents, Independent Contractors and Joint Venture Partners**

Before an independent contractor or joint venture partner may receive or be allowed to access or use CPNI for the purpose of marketing communications-related or other services to a particular customer, the Company must have obtained a signed "Opt-In CPNI Notice" (Attachment 5) from that customer.

Before an agent, independent contractor or joint venture partner may receive or be allowed to access or use the Company's CPNI, the agent's, independent contractor's or joint venture partner's agreement with the Company must contain provisions (or the Company and the agent, independent contractor or joint venture partner must enter into an additional confidentiality agreement which provides) that: (a) the agent, independent contractor or joint venture partner may use the CPNI only for the purpose for which the CPNI has been provided; (b) the agent, independent contractor or joint venture partner may not disclose or distribute the CPNI to, or allow access to the CPNI by, any other party (unless the agent, independent contractor or joint venture partner is expressly and specifically required to do so by a court order); and (c) the agent, independent contractor or joint venture partner must implement appropriate and specific safeguards acceptable to the Company to ensure the confidentiality of the Company's CPNI.

## **V. Permissible Uses of Proprietary Information Obtained from Other Carriers**

The Company may receive or obtain proprietary information (including CPNI) from other carriers for the purpose of: (a) executing changes of customer services and accounts to the other carrier; and (b) providing telecommunications services for or in conjunction with the other carrier (including services provided via interconnection, traffic exchange, reciprocal compensation, access, and bill and keep arrangements).

**The Company may use proprietary information received or obtained from other carriers only for the purpose(s) for which it is provided by the other carriers.** If there is any uncertainty regarding the purpose(s) intended by the other carrier(s), Company employees and agents are required to consult with the CPNI Compliance Officer, who will determine whether it is necessary to seek and obtain written or email confirmation of purpose(s) from the other carrier(s). Company employees and agents are expressly prohibited from using proprietary information received or obtained from other carriers for purposes not intended by such carriers (particularly for uses related to the Company's marketing of its own services, including customer retention and customer win-back efforts).

**NOTE REGARDING WIN-BACK EFFORTS:** Efforts to retain or win back customers lost in whole or part to other carriers are NOT prohibited. However, the Company's employees and others acting on the Company's behalf may not use proprietary information obtained from the competing carrier to trigger, design or execute its customer retention or win-back effort. Company employees designing and/or conducting a customer retention or win-back effort **must document** that the information they used and relied upon was obtained solely and entirely from sources other than proprietary information received or obtained from the competing carrier.

## VI. Permissible Uses of CPNI Obtained from Customers

Company employees and agents are strictly prohibited from accessing or using CPNI, and from disclosing or distributing CPNI to individuals or entities inside or outside the Company, **except** as follows:

### A. Requests for CPNI from Law Enforcement

1. The Company will provide CPNI (including call detail information) to a law enforcement agency in accordance with applicable legal requirements. Generally, such legal requirements entail an appropriate warrant or subpoena that specifies the particular CPNI to be furnished.
2. **Company employees, agents, independent contractors and joint venture partners must direct all law enforcement requests for CPNI (whether or not accompanied by a warrant or subpoena) to the CPNI Compliance Officer, who will be responsible for handling such requests and for consulting with counsel (particularly in any instances where law enforcement claims that a warrant or subpoena is not required).**

### B. Requests for CPNI from Customers or Purported Customers

1. **Telephone Requests for Call Detail Information.** When a customer or a person claiming to be a customer calls the Company to request call detail information regarding the customer over the telephone, the Company will provide the requested call detail information **only** under the following three alternative circumstances:
  - (i) the Company may provide the requested information over the telephone during the customer-initiated call if; (a) the caller provides a pre-established password that meets the requirements in paragraphs 1.a through 1.g. below; or (b) the caller correctly answers the pre-established “shared secret” questions comprising the Company’s back-up customer authentication method for that customer (if he or she loses or forgets his or her password); or
  - (ii) the Company may, at the customer’s request, send the requested call detail information to the customer’s postal or electronic “address of record”; or
  - (iii) the Company may terminate the customer-initiated call, initiate a call to the customer’s “telephone number of record” (which must be the telephone number associated with the underlying service, and may not be some other telephone number supplied as part of the contact information for the customer) and disclose the requested call detail information to the customer during the Company-initiated call.
  - a. Passwords can be designed in a manner that is privately significant and memorable to the customer (*e.g.*, “pirates1971,” “1836alamo,” “\$beatles4”). .
  - b. The Company and each customer will establish a password (and a back-up customer authentication method if the customer loses or forgets his or her password) for each new customer at the time that the customer initiates service.

c. The Company and each customer will establish a new or replacement password (and a back-up customer authentication method if the customer loses or forgets his or her password) for existing customers desiring a password pursuant to the following procedure. The Company will periodically announce on its website, in its newsletter and/or in its billing materials that customers must have a password for security and privacy purposes in order to call the Company and obtain their call detail information over the telephone. The Company announcements will inform customers that they may obtain an initial or replacement password: (i) if they come in person to the Company's business office, produce a driver's license, passport or other government-issued identification verifying their identity; or (ii) if they call a specified Company telephone number from their "telephone number of record" (see definition above) and then wait at that number until a Company employee calls them back; or (iii) if they ask the Company to send a randomly-generated Personal Identification Number ("PIN") to their "telephone number of record" (see definition above) by voice, voicemail or text message or mail it to their "address of record" (see definition above), and then call the Company back and provide the correct PIN.

d. The Company's "back-up customer authentication method" will consist of a "shared secret" combination of pre-selected questions by the Company and pre-selected answers by the customer regarding non-public aspects of the customer's life that would not be known by a pretexter, hacker or other unauthorized entity. If the customer claims to have lost or forgotten his or her password, but can correctly provide the pre-selected answers to the pre-selected "shared secret" questions, the requested call detail information can be given to the customer over the telephone during the customer-initiated call.

e. Because pretexters can replicate caller ID numbers, caller ID is not an appropriate method for authenticating a customer-initiated call requesting call detail information and may not be employed for such purpose by the Company.

f. The Company will retain all customer passwords and "shared secret" question-answer combinations in secure files that may be accessed only by authorized Company employees who need such information in order to authenticate the identity of customers requesting call detail information over the telephone. Paper copies of this information are retained in locked drawers or filing cabinets that may be accessed only by Company employees authorized to supervise or perform customer authentications. Electronic files containing this information are maintained on computers that are not accessible from the Internet or that are behind firewalls that are regularly monitored and tested for effectiveness. In addition, such electronic files may be accessed only by authorized Company employees who have been provided a currently effective password (which password is periodically changed).

g. If a customer calls the Company regarding a service or billing issue, and if the customer himself or herself (without prompting or assistance) is able to provide **all** of the call detail information necessary to address the issue (*e.g.*, the telephone number called, the date and duration of the call, and the amount charged for the call), the Company employee may proceed to address and resolve the issue during the call. However, the Company employee may not disclose to the customer any call detail information other than the call detail information provided by the customer without the customer first providing his or her password (or answering the back-up "shared secret" question-answer combinations).

2. **Telephone Requests for CPNI That Is Not Call Detail Information.** When a customer or a person claiming to be a customer calls the Company to request over the telephone CPNI regarding the customer that is not call detail information (e.g., information about the telecommunications and information services purchased by the customer), the Company employee handling the call must establish that the person calling is actually the named customer, but is not presently required by FCC Rules to have the caller furnish a pre-established password. However, given the potential sanctions imposed upon unauthorized disclosure of CPNI and the lack of FCC guidance regarding acceptable alternative methods of customer authentication, Company employees will authenticate all telephone requests for CPNI in the same manner whether or not the CPNI consists of call detail information. That is, Company employees must: (a) be furnished the customer's pre-established password (or correct answers to the pre-established back-up "shared secret" combinations); (b) send the requested information to the customer's postal or electronic "address of record" (see definition above); or (c) call the customer back at the customer's "telephone number of record" (see definition above) with the requested information.
3. **Customer In-Bound Marketing Calls.** When an existing customer calls the Company to inquire about or order new, additional or modified services (in-bound marketing), the Company employee may use the customer's CPNI to assist the customer for the duration of the customer's call ONLY under the following circumstances:

If the Company employee must disclose call detail information or other CPNI to the customer during the call, the employee must: (i) require the caller to establish his or her identity by providing a pre-established password (or the answers to the back-up "shared secret" customer authentication questions); (ii) provide the customer with the oral notice set forth in Attachment 3; and (iii) obtain the customer's oral consent to the use of his or her CPNI during the call, complete the "Oral Inbound Marketing CPNI Notice (Attachment 3 to this manual) and place it in the appropriate Company CPNI compliance file.

4. **Written Requests for CPNI.** Upon receiving an appropriate written request from a customer, the Company will provide to the customer or to any person designated by the customer a written document containing specifically requested portions of the customer's CPNI. Any and all such customer requests: (1) must be made in writing; (2) must include the customer's correct billing name and address and telephone number; (3) must specify exactly what type or types of CPNI are to be provided; (4) must specify the time period for which the CPNI must be provided; (5) must be signed by the customer; and (6) will be mailed to the customer's most recent address in our records. A "Customer CPNI Request Form" is included as Attachment 6.

If the customer requests to pick-up the requested CPNI in person at the Company's business office, the customer must produce a driver's license, passport or other government-issued identification verifying his or her identity. CPNI will be provided in person only to the customer of record, and will not be provided to any other individuals, including individuals claiming to be the customer's agent or relative.

In all other cases (including instances where the customer making the written request cannot produce acceptable government-issued identification written documents containing specifically requested portions of the customer's CPNI will be sent to the customer's established "address of record" (see definition above) by United States mail or other secure and reliable delivery service (e.g., Federal Express or UPS).

When a customer submits a written request for the delivery of his or her CPNI to a third party (and ALL such requests must be in writing), the Company will call the customer's "telephone number of record" (see definition above) and/or send a notification of the customer's request to the customer's "address of record" (see definition above) to verify the accuracy of this request. This is a sensitive area that may place the Company in the middle of potentially conflicting FCC and statutory policies seeking to protect customers from unauthorized distribution of their CPNI and seeking to enable competing carriers to obtain rapid access to the CPNI of new and potential new customers. Any questions or concerns regarding the validity of a written request by a "customer" for delivery of CPNI to a third party must be brought immediately to the attention of the CPNI Compliance Officer. It is the preference of the Company that in such instances, the requested CPNI be provided directly to the customer, who is then free to deliver it to the desired third party. However, if the customer cannot be persuaded to follow this course, the procedures in this paragraph should be followed.

5. **In-Person Request at Business Office or Retail Location.** A "customer of record" (i.e., a customer whose name is on the account) may review and/or obtain copies of his or her CPNI at any Company business office or retail sales location where such CPNI is available by coming in-person to the facility and presenting a driver's license, passport or other government-issued identification that verifies his or her identity.
6. **Business Customer Exception.** The Company may contract with certain multi-line business customers for different procedures to handle the business customer's requests for CPNI. Such alternative procedures must be reviewed by the CPNI Compliance Officer and counsel before they are implemented. At minimum, the alternative procedures require the Company to assign an employee as the dedicated account representative with primary responsibility for handling all CPNI requests from the business customer.
7. **Adult Children of Elderly Customers.** The Company is aware that adult children (or other relatives) of elderly customers may have legitimate needs to make service changes or to raise and resolve billing questions on behalf of their parents. At the same time, the Company has concerns that a pretexter might pose as an "adult child" in order to gain unauthorized access to an elderly customer's CPNI, or that a family member may simply be unauthorized to receive the customer's CPNI. The Company will normally respond to such requests by requiring the adult relative to either furnish proof that he or she is authorized by the customer to transact such business (through a legally binding power of attorney or other recognized legal document). If applicable, the adult child should provide **all** of the call detail information necessary to address the issue. If that approach is not feasible in a particular instance, the matter must be brought to the attention of the CPNI Compliance Officer who may devise (in consultation with counsel, if necessary) a solution that will satisfy the elderly customer's legitimate service needs without risking the unauthorized disclosure of the customer's CPNI, and place a memorandum describing the particular circumstances and solution in the Company's CPNI files.

### **C. Requests for CPNI from Competing Carriers and Other Third Parties**

1. Because of the danger of unauthorized access to CPNI, the Company will not accept, process or fulfill written or verbal requests by any third party (other than a recognized law enforcement agency as set forth in Section VI.A above) for a customer's CPNI. This

restriction encompasses requests for a customer's CPNI by a competing carrier, including a competing carrier that claims to be an existing or former customer's new carrier.

2. A customer may request in writing that his or her CPNI be delivered to a competing carrier or other third party. If the written request is presented by the customer in person at the Company's business office, the Company will fulfill it if the customer presents a driver's license, passport or other government-issued identification that verifies his or her identity. If the written request is received via U.S. mail or other recognized delivery service, the Company will call the customer's "telephone number of record" (see definition above) and/or send a notification of the customer's request to the customer's "address of record" (see definition above) to verify the accuracy of this request. As noted in Section VI.B.4 above, this is a sensitive area that may place the Company in the middle of potentially conflicting FCC and statutory policies regarding CPNI protection and telecommunications competition. Any questions or concerns regarding the validity of a written request by a "customer" for delivery of CPNI to a competing carrier or other third party must be brought immediately to the attention of the CPNI Compliance Officer. It is the preference of the Company that in such instances, the requested CPNI be provided directly to the customer, who is then free to deliver it to the desired third party. However, if the customer cannot be persuaded to follow this course, the procedures in this paragraph should be followed.

#### **D. Use of CPNI for Marketing Purposes**

1. **Marketing Activities Not Involving CPNI.** Marketing activities that do not use CPNI are not restricted in any manner by the federal CPNI requirements. The Company's employees, independent contractors and joint venture partners may send direct mail advertisements to households and businesses in various geographic areas (including communities, neighborhoods and zip codes) as long as they do not use CPNI to design the direct mail campaign or to target particular recipients. Such direct mail advertisements may be included as inserts in the monthly bills sent to the Company's customers, as long as CPNI is not used to target particular customers or to provide particular bill inserts to particular customers. The Company's employees, independent contractors and joint venture partners may also engage in telemarketing (subject to do-not-call list restrictions) to households and businesses in particular communities or exchange areas, as long as CPNI is not used to target particular recipients or to design the particular script or message transmitted to particular recipients. **IT IS THE OFFICIAL POLICY OF THIS COMPANY THAT CPNI WILL NOT BE USED IN MARKETING CAMPAIGNS.**
  - a.. CPNI may be used, without customer approval, to provide or market "adjunct-to-basic" services to a customer subscribing to the underlying basic service (*e.g.*, services such as speed dialing, computer-provided directory assistance, call monitoring, call tracing, call blocking, call return, repeat dialing, call tracking, call waiting, caller ID, call forwarding, and certain Centrex features are "adjunct" to basic local exchange service).
  - b. CPNI may be used, without customer approval, to provide or market services "necessary to" or "used in" the provision of the telecommunications service from which the CPNI is derived (*e.g.*, CPNI may be used to provide or market installation, maintenance, and repair functions with respect to the customer's services).

**CAUTION: Because the services that are “necessary to” or “used in” the provision of a category of telecommunications service may be subject to varying interpretation, Company employees must consult with the Company’s CPNI Compliance Officer before using CPNI, without customer approval, to provide or market new services under this classification.**

c. If a customer takes multiple categories of service from the Company (*e.g.*, local exchange, long distance toll, and cellular service), the scope of the Company’s permissible use of the customer’s CPNI, without customer approval, expands accordingly. For example, if the Company provides local exchange service and long distance toll service to a customer, its employees can use the customer’s CPNI from these services to design and market various packages of local exchange and toll services to the customer.

d. **SPECIAL FCC LEC/IXC RULE:** If the Company provides local exchange or interexchange services, its employees may use, disclose, or permit access to CPNI derived from its provision of local exchange service or interexchange service, without customer approval, to provide customer premises equipment (“CPE”), call answering, voice mail or messaging, voice storage and retrieval services, fax store and forward, and protocol conversion.

e. **SPECIAL FCC CMRS RULE:** If the Company provides wireless service, its employees may use, disclose, or permit access to CPNI derived from its provision of Commercial Mobile Radio Services, without customer approval, to provide customer premises equipment (“CPE”) and information services.

f. **GRAY AREA:** Some services, *e.g.*, digital subscriber line (“DSL”) services offered by local exchange carriers, pose difficult questions that are not yet clearly resolved by FCC precedent. DSL services are furnished over the same customer loops as local exchange service, and can be argued to be part of the same “category” or “package” of services as local exchange service. On the other hand, DSL services have been classified as interstate services (as opposed to local exchange services which are primarily intrastate services), and are often associated with the delivery of Internet access and video services that are not local exchange services. Before using CPNI derived from the provision of local exchange service, without customer approval, to provide or market DSL services, the Company’s employees must consult with the CPNI Compliance Officer, who (in turn) should consult with counsel.

3. **Customer-Initiated (In-Bound) Marketing Calls.** When an existing customer calls the Company to inquire about or order new, additional or modified services (in-bound marketing), the Company’s employee may use the customer’s CPNI to assist the customer for the duration of the customer’s call **ONLY** under the following circumstances:

If the Company employee must disclose call detail information or other CPNI to the customer during the call, the employee must: (i) require the caller to establish his or her identity by providing a pre-established password (or the answers to the back-up “shared secret” customer authentication questions); (ii) provide the customer with the oral notice set forth in Attachment 3; and (iii) obtain the customer’s oral consent to the use of his or her CPNI during the call, complete the “Oral Inbound Marketing CPNI Notice

(Attachment 3 to this manual) and place it in the appropriate Company CPNI compliance file.

#### **SECTION D.4**

**UNTIL FURTHER NOTICE IT IS THE OFFICIAL POLICY OF THIS COMPANY THAT CPNI WILL NOT BE USED IN MARKETING CAMPAIGNS. THE INFORMATION PROVIDED IN THIS SECTION D.4 IS INFORMATIONAL ONLY TO DEMONSTRATE THE RESTRICTED NATURE OF CPNI USE IN MARKETING CAMPAIGNS.**

4. **Use of CPNI for Company-Initiated (Out-Bound) Marketing Purposes.** The Company uses, discloses, and/or permits access to CPNI in connection with Company-initiated marketing of services to which a customer does not already subscribe from the Company (out-bound marketing) only pursuant to the notice and approval procedures set forth in Sections 64.2007, 64.2008, and 64.2009 of the FCC's Rules.

a. All out-bound marketing activities and campaigns must be reviewed by the Company's CPNI Compliance Officer for compliance with the CPNI restrictions and requirements in the Communications Act and the FCC Rules, and approved by the CPNI Compliance Officer before they can commence. Company employees, independent contractors and joint venture partners proposing or designing an out-bound marketing campaign that may use CPNI should initiate this CPNI review and approval process as early as possible, for review (plus the potential need to obtain customer approvals for the proposed CPNI use) may take several months.

b. The Company maintains appropriate paper and/or electronic records that allow its employees, independent contractors and joint venture partners to clearly establish the status of each customer's Opt-out and/or Opt-In approvals (if any) prior to use of the customer's CPNI. These records include: (i) the date(s) of any and all of the customer's deemed Opt-out approvals and/or Opt-in approvals, together with the dates of any modifications or revocations of such approvals; and (ii) the type(s) of CPNI use, access, disclosure and/or distribution approved by the customer.

c. Before a customer's CPNI can be used in an out-bound marketing activity or campaign, the Company's records must be checked to determine the status of the customer's CPNI approval. Company employees, agents, independent contractors and joint venture partners are required to notify the CPNI Compliance Officer of any access, accuracy or security problems they encounter with respect to these records.

d. If new, additional or extended approvals are necessary, the CPNI Compliance Officer will determine whether the Company's "Opt-Out CPNI Notice" (Attachment 4) or "Opt-In CPNI Notice" (Attachment 5) must be used with respect to various proposed out-bound marketing activities.

e. The Opt-Out mechanism is required for customer approval: (i) when the Company uses CPNI to market services that are NOT within the same "category" or "package" of services to which the customer presently subscribes from the Company; and (ii) when the Company discloses CPNI to affiliates that provide communications-related services. A customer is deemed to have provided appropriate "opt-out approval" by failing to object to the Company's "Opt-Out CPNI Notice" (Attachment 4) for at least thirty-three

(33) days after notice was mailed or emailed to the customer. A customer's deemed "opt-out approval" is effective for a maximum of two (2) years, and may be revoked by the customer at any time during that period.

f. The Opt-In mechanism is required for customer approval: (i) before the Company discloses CPNI to independent contractors or joint venture partners for any marketing purposes; and (b) before the Company discloses CPNI to affiliates that DO NOT provide communications-related services. A customer has provided appropriate "opt-in approval" only if he or she has returned an appropriately executed copy of the Company's "Opt-In CPNI Notice" (Attachment 5). A customer's "opt-in approval" is effective until it is revoked or modified by the customer.

g. Company employees are strictly required to check the proper Company files and customer records to determine whether a particular customer has given his or her proper and required "opt-in approval" or "opt-out approval" for a particular disclosure, distribution or access to CPNI for marketing purposes, and whether such approval is still effective. Employees are cautioned that some customer approvals (as well as some Opt-In or Opt-Out Notices) may have a very narrow scope, and may not encompass a desired use. Employees are prohibited from making their own judgment calls to resolve uncertainties and ambiguities, and will bear the risk of disciplinary action if they do so and are wrong. Rather, employees are required to bring uncertainties and ambiguities to the attention of the Company's CPNI Compliance Officer for appropriate resolution.

h. The CPNI Compliance Officer will maintain a record of each out-bound marketing activity or campaign, including: (i) a description of the campaign; (ii) the specific CPNI that was used in the campaign; (iii) the date and purpose of the campaign; and (iv) what products and services were offered as part of the campaign. This record shall be maintained for a minimum of two years.

i. Employees, agents, independent contractors or joint venture partners must notify the CPNI Compliance Officer within 24 hours of any instance where the Opt-Out mechanism does not work properly (*e.g.*, where a customer claims that he or she never received an Opt-Out CPNI Notice, or where the customer claims that he or she returned an Opt-Out CPNI Notice denying his or her approval of the proposed CPNI use). The notification shall include a description of the Opt-Out mechanism used, the problems experienced, and a copy of the Opt-Out CPNI Notice provided to customers.

j. The CPNI Compliance Officer must provide written notice to the FCC within five (5) business days of any instance where the Opt-Out mechanism did not work properly.

## **SECTION D.5**

**5. Sharing of CPNI With Affiliates.** The Company will allow the CPNI for particular customers of the Company's telecommunications services to be accessed or used by, or disclosed or distributed to, an Affiliate (that is, a separate corporation, partnership or other entity that is owned in whole or part by the Company or by the owners of the Company), subject to appropriate limitations and customer approval procedures.

a. If the Company and Affiliate already provide a group or bundled package of related telecommunications services to a particular customer (for example, local exchange telephone service and long distance toll service), the Company and Affiliate may share

the customer's CPNI without obtaining the customer's approval in order to market services within the scope of the group or bundled package of services already provided. [For example, an ILEC that provides local exchange service to a customer, and its IXC affiliate providing toll services to that customer, may use the customer's CPNI without approval to market various bundled packages of local and toll service to the customer.]

b. If the Affiliate offers or provides communications-related services (including certain information services containing telecommunications elements), the Company may disclose, distribute, or permit access by the Affiliate to the Company's CPNI for a particular customer ONLY IF the customer is deemed to have provided appropriate "opt-out approval" by failing to object to the Company's "Opt-Out CPNI Notice" (Attachment 4) for at least thirty-three (33) days after notice was mailed or emailed to the customer. A customer's deemed "opt-out approval" is effective for a maximum of two (2) years, and may be revoked by the customer at any time during that period.

c. If the Affiliate does not provide communications-related services (for example, it provides cable television service or sells insurance policies), the Company's employees may disclose, distribute, or permit access by the Affiliate to the Company's CPNI for a particular customer ONLY IF the customer has provided appropriate "opt-in approval" by returning an appropriately executed copy of the Company's "Opt-In CPNI Notice" (Attachment 5). A customer's "opt-in approval" is effective until it is revoked or modified by the customer.

**NOTE:** Company employees are strictly required to check the proper Company files and customer records to determine whether a particular customer has given his or her proper and required "opt-in approval" or "opt-out approval" for a particular disclosure, distribution or access to CPNI to an Affiliate, and whether such approval is still effective. Employees are cautioned that some customer approvals (as well as some Opt-In or Opt-Out Notices) may have a very narrow scope, and may not encompass a desired use. Employees are strongly discouraged from making their own judgment calls to resolve uncertainties and ambiguities, and will bear the risk of disciplinary action if they do so and are wrong. Rather, employees are urged to bring uncertainties and ambiguities to the attention of the Company's CPNI Compliance Officer for appropriate resolution.

**NOTE FURTHER:** Employees who split their working time between the Company and an Affiliate may not access, use, disclose or distribute the Company's CPNI when performing any task for or on behalf of the Affiliate, unless the customer has given the appropriate "opt-out approval" or "opt-in approval."

## **E. Use of CPNI for Billing and Administrative Purposes**

1. **Billing and Collection.** The Company's employees and billing agents may use CPNI to initiate, render, bill and collect for telecommunications services. The Company may obtain information from new or existing customers that may constitute CPNI as part of applications or requests for new, additional or modified services, and its employees and agents may use such customer information (without further customer approval) to initiate and provide the services. Likewise, the Company's employees and billing agents may use customer service and calling records (without customer approval): (a) to bill customers for services rendered to them; (b) to investigate and resolve disputes with

customers regarding their bills; and (c) to pursue legal, arbitration, or other processes to collect late or unpaid bills from customers.

2. **Fraud and Abuse.** The Company's employees and agents (including its attorneys) may use CPNI without customer approval to protect the Company's rights or property, and to protect users and other carriers from fraudulent, abusive or illegal use of (or subscription to) the telecommunications service from which the CPNI is derived.

**NOTE:** Because allegations and investigations of fraud, abuse and illegal use constitute very sensitive matters, any access, use, disclosure or distribution of CPNI pursuant to this Section E.2 must be expressly approved in advance and in writing by the Company's CPNI Compliance Officer.

3. **Prohibition Against Anti-Competitive and Personal Uses.**

- a. The Company's employees, agents, independent contractors and joint venture partners may **NOT** use CPNI to identify or track customers who have made calls to, or received calls from, competing carriers.

- b. The Company's employees, agents, independent contractors or joint venture partners may not use or disclose CPNI for personal reasons or for their personal profit (*e.g.*, to determine whether a spouse is calling or receiving calls from certain persons). Any such personal use or disclosure of CPNI may result in immediate termination or suspension.

**F. Security of CPNI Files:** Company policy mandates that

1. Files containing CPNI must be maintained in a secure manner such that they cannot be used, accessed, disclosed or distributed by unauthorized individuals or in an unauthorized manner.
2. Paper files containing CPNI must be kept in locked drawers or locked file cabinets in secure areas, and may not be used, removed, or copied in an unauthorized manner.
3. Electronic files and databases containing CPNI must be maintained on computers that are not accessible from the Internet or that are on the Company's intranet behind firewalls that are regularly monitored and tested for effectiveness. In addition, such electronic files and databases may be accessed only by authorized Company employees who have been provided a currently effective strong login ID and password (which password is periodically changed).
4. Company employees, agents, independent contractors and joint venture partners are required to notify the CPNI Compliance Officer immediately by telephone or email, and to provide a detailed written follow-up memorandum within no more than five (5) business days, of any access or security problems they encounter with respect to files containing CPNI.
5. The Company must take reasonable measures to discover and protect against activity that is indicative of pretexting including requiring Company employees and agents to notify the CPNI Compliance Officer immediately by voice, voicemail or email of: (a) any suspicious or unusual call requesting a customer's call detail information or other CPNI (including a call where the caller furnishes an incorrect password or incorrect

answer to one or both of the “shared secret” question-answer combinations); (b) any suspicious or unusual attempt by an individual to change a customer’s password or account information (including providing inadequate or inappropriate identification or incorrect “address or record,” “telephone number of record” or other significant service information); (c) any and all discovered instances where access to the Company’s electronic files or databases containing passwords or CPNI was denied due to the provision of incorrect logins and/or passwords; and (d) any complaint by a customer of unauthorized or inappropriate use or disclosure of his or her CPNI. The CPNI Compliance Officer will request further information in writing, and investigate or supervise the investigation of, any incident or group of incidents that reasonably appear to entail pretexting.

## **G. Security of Online Accounts**

1. The Company may permit its customers to establish online accounts, but must require an appropriate password to be furnished by the customer before he or she can access any CPNI in his or her online account.
2. Customers may obtain an initial or replacement password: (i) if they come in person to the Company’s business office, produce a driver’s license, passport or other government-issued identification verifying their identity, and correctly answer certain questions regarding their service and address; or (ii) if they call a specified Company telephone number from their telephone number of record, and then wait at that number until a Company representative calls them back and obtains correct answers to certain questions regarding their service and address.

## **VII. Required Certifications and Notices**

1. **Annual Section 64.2009(e) Certification.** The Company must file with the FCC’s Enforcement Bureau in EB Docket No. 06-36, on or before March 1 of every year (starting in 2008), an annual Section 64.2009(e) certification of compliance with the FCC’s CPNI Rules (47 C.F.R. §§64.2001 through 64.2011) during the previous calendar year.

a. The annual Section 64.2009(e) certification must be signed by an Officer of the Company as an agent of the Company. The Officer must state specifically 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 FCC’s CPNI Rules (47 C.F.R. §§64.2001 through 64.2011).”

b. The certification must be accompanied by a separate statement explaining how the Company’s operating procedures ensure that it is in compliance with the FCC’s CPNI Rules.

c. The certification must also be accompanied by a separate statement describing and explaining any actions taken by the Company against data brokers during the previous calendar year, or by a separate statement indicating why the Company took no actions against data brokers during the previous calendar year (*e.g.*, because, to the best of the Company’s knowledge, no data broker attempted to obtain any call detail information or other CPNI from the Company during the year).

d. The certification must be accompanied by a separate summary of all customer complaints

received by the Company during the previous calendar year concerning the unauthorized release of CPNI.

e. A model annual Section 64.2009(e) certification is included as Attachment 7.

2. **Section 64.2009(c) Marketing Record.** The Compliance Officer will maintain a record of each out-bound marketing activity or campaign that used CPNI, including:

a. a description of the campaign;

b. the specific CPNI that was used in the campaign;

c. the date and purpose of the campaign;

d. the name and relationship of any third party to which CPNI was disclosed or provided, or which was allowed to access CPNI; and

e. what products and services were offered as part of the campaign.

This record shall be retained in the Company's files for a minimum of two years.

3. **Section 64.2010(f) Notice to Customers of Account Changes.** The Company will notify customers immediately of certain changes in their accounts that may affect privacy or security matters.

a. The types of changes that require immediate notification include: (i) change or request for change of the customer's password; (ii) change or request for change of the customer's address of record; (iii) change or request for change of any significant element of the customer's online account; and (iv) a change or request for change to the customer's responses with respect to the back-up means of authentication for lost or forgotten passwords.

b. The notice may be provided by: (i) a Company call or voicemail to the customer's telephone number of record; (ii) a Company text message to the customer's telephone number of record; or (iii) a written notice mailed to the customer's address of record (to the customer's prior address of record if the change includes a change in the customer's address of record).

c. The notice must identify only the general type of change and must not reveal the changed information.

4. **Section 64.2011 Notice of CPNI Security Breach.** The Company must provide an initial notice to law enforcement and a subsequent notice to the customer if a security breach results in the disclosure of the customer's CPNI to a third party without the customer's authorization.

a. As soon as practicable (and in no event more than seven (7) days) after the Company discovers that a person (without authorization or exceeding authorization) has intentionally gained access to, used or disclosed CPNI, the Company must provide electronic notification of such breach to the United States Secret Service and to the Federal Bureau of Investigation via a central reporting facility accessed through a link maintained by the FCC.

b. Generally, the Company may not notify Company customers or disclose the security breach to the news media or public for seven (7) full business days after it provides notice to the United States Secret Service and to the Federal Bureau of Investigation. This “black-out period” is considered very important by the FCC and law enforcement for the success of potential or ongoing criminal and national security investigations, and premature customer notifications or public disclosures may be severely punished. Moreover, law enforcement has the right to direct the Company to extend the “black-out period” as long as necessary to protect or facilitate its investigation.

c. If the Company believes that there is an extraordinary and urgent need to notify any class of affected customers before the end of the relevant “black-out period” in order to avoid immediate and irreparable harm, the Company’s CPNI Compliance Officer will consult with counsel and with the relevant law enforcement agency investigating the security breach. The Company may provide notice to the class of affected customers only: (i) if the relevant law enforcement agency agrees; and (ii) pursuant to any and all conditions, restrictions and prohibitions established by such law enforcement agency regarding such notice.

d. As soon as practicable after the incident, the Company must maintain a record of each discovered CPNI security breach, including: (i) the date of discovery of the breach; (ii) the date, time and content of the electronic notice sent to the United States Secret Service and to the Federal Bureau of Investigation; (iii) correspondence with the relevant law enforcement agency regarding any extensions of the “black-out period”; (iv) the date, time and content of the notification(s) sent to the Company’s customers; (v) a detailed description of the CPNI that was the subject of the breach; and (vi) a detailed description of the circumstances of the breach. Each such record must be retained by the Company for at least two years after it is completed and placed in the Company’s files.

## **VIII. Disciplinary Procedures**

The Company considers compliance with the Communications Act and FCC Rules regarding the use, disclosure, and access to CPNI to be of the utmost importance.

Violation by Company employees and agents of such CPNI requirements will lead to prompt disciplinary action (up to and including remedial training, reprimands, unfavorable performance reviews, probation, and termination), depending upon the circumstances of the violation (including the severity of the violation, whether the violation was a first time or repeat violation, whether appropriate guidance was sought or received from the CPNI Compliance Officer, and the extent to which the violation was or was not deliberate or malicious).

Violation by Company independent contractors or joint venture partners of such CPNI requirements will lead to prompt disciplinary action (up to and including remedial training, termination of the contract and/or other remedial legal actions).

Company employees, agents, independent contractors and joint venture partners are also cautioned about the dangers of both inadvertent and intentional cooperation with pretexters. In the wake of the improper provision or sale of CPNI to certain Internet sites, the FCC has made it clear that it will impose swift and potentially severe sanctions upon companies that violate its CPNI requirements. The FCC has stated that it expects carriers to take “every reasonable precaution” to protect the confidentiality of proprietary and personal customer information, and has put carriers on notice that it will infer from evidence that a pretexter obtained access to a customer’s CPNI that the carrier did not sufficiently protect that customer’s CPNI. The carrier

will then have the burden of demonstrating to the FCC that it took reasonable steps to protect CPNI from unauthorized disclosure (in light of the threat posed by pretexting and the sensitivity of the customer information at issue) if it is to escape forfeitures or other sanctions.

Pretexters may use a variety of tactics to try to fool telephone company representatives in order to get unauthorized and unlawful access to CPNI. Some of these tactics involve mock anger and bullying; others entail pleading and playing upon normal human emotions. Company representatives that have spent years learning to be helpful to customers need also to learn to follow customer authentication procedures very carefully and completely. Company employees, agents, independent contractors and joint venture partners who cut corners on customer authentication procedures will be disciplined and/or reassigned to positions where they will not have contact with potential pretexters.

In some unfortunate instances, pretexters have obtained CPNI from telecommunications company representatives who have cooperated for friendship, financial or other reasons. The Company will take any and all disciplinary, termination and/or remedial actions permitted by applicable federal and state employment law against any Company representative that is reasonably suspected to have cooperated knowingly and intentionally with a pretexter.

**ATTACHMENT 1**

**SCRIPT AND FORM FOR  
ORAL INBOUND MARKETING CPNI NOTICE**

This Notice must be used to obtain a customer's oral approval for use of his or her CPNI for the duration of a single incoming call from the customer to inquire about or order new or additional services outside of his or her existing category or package of services.

**ORAL INBOUND MARKETING CPNI NOTICE (EXAMPLE)**

It is possible that I can better assist you on this call if I can access and use certain of your existing account records known as CPNI. However, before I can do so, federal law requires me to read you a notice and give you the option of approving or disapproving my use of your records during this call. May I read you the Notice?

If "no," proceed to assist the customer without using his or her CPNI.

If "yes," proceed to read the Notice:

CPNI (which stands for Customer Proprietary Network Information) consists of the call, service and billing records regarding your use of the telecommunications services that you purchase from us (e.g., the telephone numbers you call; the frequency, timing and duration of your calls; and the telecommunications and information services you purchase).

You have a right to the confidentiality of your CPNI, and the Company has a duty, under federal law, to protect that confidentiality. You have a right to approve or disapprove my use of your CPNI to assist you on this call.

If you approve, I may be better able to assist you during this call. Your approval will be limited to this call.

If you disapprove, I will continue to assist you to the best of my ability, but I will not be able to access or use your CPNI records during this call.

Would you like to approve or disapprove?

If the customer approves, complete this form and deliver it to the CPNI Compliance Officer as soon as possible.

---

The named customer approved the use of CPNI during a call on the specified date.

Customer Name \_\_\_\_\_ Telephone Number \_\_\_\_\_

Company Representative \_\_\_\_\_ Date \_\_\_\_\_

## ATTACHMENT 2

### OPT-OUT CPNI NOTICE

**INFORMATIONAL ONLY: UNTIL FURTHER NOTICE IT IS THE OFFICIAL POLICY OF THIS COMPANY THAT CPNI WILL NOT BE USED IN MARKETING CAMPAIGNS.**

This Notice must be used to obtain customer approval to use CPNI for out-bound marketing campaigns, and to provide or share CPNI with affiliates that provide communications-related services.

The Notice may be sent to customers in a variety of ways, including by separate mail, as a bill insert, by facsimile, or by email. The attached model Notice assumes that it will be sent by mail or as a bill insert.

Customers must be allowed to disapprove by a method or variety of methods that impose no additional cost upon the customer and that are available 24 hours a day. The attached model Notice assumes that disapprovals will be made by mail, facsimile or telephone call.

Because no response by a customer to an Opt-Out Notice within 33 days after it is sent is deemed to constitute the customer's approval of the proposed CPNI use, the FCC requires the company to take substantial measures to ensure that Opt-Out Notices are received, read and understood by customers.

The Notice must be comprehensible to the ordinary customer, and must not be misleading. It must be clearly legible, use sufficiently large type, and be delivered in a manner so as to be readily apparent to the customer. If any portion of the Notice is translated into another language, the entire Notice must be translated into that language.

If email is used to deliver an Opt-Out Notice, there are substantial additional requirements and precautions, including: (a) customers must give their express prior approval for CPNI notices to be sent to them via email; (b) customers must be allowed to reply directly to the email to disapprove the proposed CPNI use; (c) email notices returned as undeliverable must be sent by an alternative means (and the 33-day clock reset); and (d) the subject line of the email must clearly and accurately identify its purpose.

The Notice must specify the entities that will receive the CPNI and the purpose(s) for which it will be used.

Some examples of the proposed use to be inserted in the third paragraph:

The Company is requesting your approval to

... use your CPNI to develop and market new video services for you.

... allow its long distance affiliate XYZ Company to access and use your CPNI to design and develop new toll services and packages for you.

**OPT-OUT CPNI NOTICE (EXAMPLE)**

[NAME OF CARRIER] is requesting your approval to access, use, disclose, or distribute your Customer Proprietary Network Information (or "CPNI") for certain purposes.

CPNI consists of the call, service and billing records regarding your use of the telecommunications services that you purchase from us (e.g., the telephone numbers you call; the frequency, timing and duration of your calls; and the telecommunications and information services you purchase).

The Company is requesting your approval to \_\_\_\_\_

\_\_\_\_\_  
[SEE EXAMPLES ON INTRODUCTORY PAGE].

You have a right to the confidentiality of your CPNI, and the Company and other carriers have a duty, under federal law, to protect that confidentiality. You have a right to approve or disapprove the proposed access, use, disclosure and/or distribution of your CPNI.

If you approve, the Company may be better able to offer products and services tailored to your needs. Your approval will be valid for up to two years, but you may revoke or limit it at any time by notifying the Company in writing that you are doing so.

If you disapprove, it will not affect the provision to you of any of the existing services which you purchase from the Company. However, we will not be able to use your CPNI to develop and offer to you new or additional services or service packages. Your disapproval will remain in effect until you revoke or limit it, which you may do in writing at any time.

If you are willing to give the Company your approval for the proposed use of your CPNI, you need do nothing further. Your approval will be deemed to have been granted thirty-three (33) days after this notice was sent to you.

If you do not approve the proposed use of your CPNI, you need to sign and date the box below and return it to the Company in the enclosed envelope, or fax it to the Company at \_\_\_\_\_, or telephone the company at the following toll-free number \_\_\_\_\_.

\_\_\_\_\_  
I have read this OPT-OUT CPNI NOTICE, and DO NOT approve of the proposed use of CPNI for the customer account specified below.

Customer Name \_\_\_\_\_ Telephone Number \_\_\_\_\_

Customer Billing Address \_\_\_\_\_

Signature \_\_\_\_\_

Printed Name \_\_\_\_\_ Date \_\_\_\_\_

## ATTACHMENT 3

### OPT-IN CPNI NOTICE

This Notice must be used to obtain customer approval to provide or share CPNI with independent contractors, joint venture partners and with affiliates that do not provide communications-related services.

The Notice may be sent to customers in a variety of ways, including by separate mail, as a bill insert, by facsimile, or by email. The attached model Notice assumes that it will be sent and returned by mail or facsimile.

The Notice must be comprehensible to the ordinary customer, and must not be misleading. It must be clearly legible, use sufficiently large type, and be delivered in a manner so as to be readily apparent to the customer. If any portion of the Notice is translated into another language, the entire Notice must be translated into that language.

The Notice must specify the entities that will receive the CPNI and the purpose(s) for which it will be used.

Some examples of the proposed use to be inserted in the third paragraph:

The Company is requesting your approval to

... allow its affiliate XYZ Company to access and use your CPNI to design and develop new services for you.

... allow its affiliate XYZ Company to access and use your CPNI to design and develop new remote banking services for you.

...allow its affiliates XYZ Company and XYZ Cable, Inc. to access and use your CPNI to market new services to you.

... disclose and distribute your CPNI to ABC Company, an entity that is not related to the Company, so that it may develop and market information service to you.

**OPT-IN CPNI NOTICE (EXAMPLE)**

[NAME OF CARRIER] is requesting your approval to access, use, disclose, or distribute your Customer Proprietary Network Information (or "CPNI") for certain purposes.

CPNI consists of the call, service and billing records regarding your use of the telecommunications services that you purchase from us (e.g., the telephone numbers you call; the frequency, timing and duration of your calls; and the telecommunications and information services you purchase).

The Company is requesting your approval to \_\_\_\_\_

---

**[SEE EXAMPLES ON INTRODUCTORY PAGE].**

You have a right to the confidentiality of your CPNI, and the Company and other carriers have a duty, under federal law, to protect that confidentiality. You have a right to approve or disapprove the proposed access, use, disclosure and/or distribution of your CPNI.

If you approve, the Company may be better able to offer products and services tailored to your needs. Your approval will be valid until you affirmatively revoke or limit it, which you may do in writing at any time.

If you disapprove, it will not affect the provision to you of any of the existing services which you purchase from the Company. However, we will not be able to allow \_\_\_\_\_ [NAME OF ENTITY SPECIFIED ABOVE] to use your CPNI to develop and offer to you new or additional services or service packages. Your disapproval will remain in effect until your revoke or limit it, which you may do in writing at any time.

If you are willing to give the Company your approval for the proposed use of your CPNI, you will need to sign and date the box below and return this Notice to the Company in the enclosed envelope, or fax it to the Company at \_\_\_\_\_. If you do not sign and return this Notice, you will be deemed to have disapproved of the proposed use of your CPNI.

---

I have read this OPT-IN CPNI NOTICE, and approve of the proposed use of CPNI for the customer account specified below. I am authorized to give approval with respect to this account.

Customer Name \_\_\_\_\_ Telephone Number \_\_\_\_\_

Customer Billing Address \_\_\_\_\_

Signature \_\_\_\_\_

Printed Name \_\_\_\_\_ Date \_\_\_\_\_

**ATTACHMENT 4**

**CUSTOMER CPNI REQUEST FORM**

Customer Name \_\_\_\_\_ Date \_\_\_\_\_

Billing Address \_\_\_\_\_  
\_\_\_\_\_

Telephone Number \_\_\_\_\_

CPNI Records Requested \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

Time Period(s), if applicable \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

Deliver CPNI Records to Customer via:  
(check one) U.S. Mail  Email  Customer Will Pick Up

If via email, specify email address \_\_\_\_\_  
(NOTE: The Company will call your telephone number of record to verify the accuracy of this email address)

Deliver CPNI Records to Third Party:  
Name and Address of Third Party:

(NOTE: The Company will call your telephone number of record and/or send a notification of the request to your address of record, to verify the accuracy of this request)

Customer Signature \_\_\_\_\_ Date \_\_\_\_\_

**ATTACHMENT 5**

**CPNI COMPLIANCE CERTIFICATE  
[Section 64.2009(e) of FCC Rules]**

**EB DOCKET NO. 06-36**

I hereby certify that I am an Officer of \_\_\_\_\_,  
and am executing this CPNI Compliance Certificate as its agent.

I have personal knowledge that the Company has established operating procedures that are adequate to ensure compliance with the Customer Proprietary Network Information rules and requirements in Subpart U of Part 64 of the Federal Communications Commission's Rules (47 C.F.R. §§64.2001 through 64.2011).

The "Statement Explaining How the Company's Operating Procedures Ensure Compliance With the FCC's CPNI Rules" attached as Exhibit 1 explains how the Company's operating procedures ensure that it is in compliance with the foregoing FCC rules during the subject Calendar Year.

The "Statement of Actions Taken Against Data Brokers" attached as Exhibit 2 describes any actions taken by the Company against data brokers during the subject Calendar Year.

The "Summary of Customer Complaints Regarding Unauthorized Release of CPNI" attached as Exhibit 3 lists the numbers of various types of customer complaints received by the Company during the subject Calendar Year concerning the unauthorized use of CPNI.

I am making this certification for Calendar Year \_\_\_\_\_.

\_\_\_\_\_  
Signature

\_\_\_\_\_  
Printed Name

\_\_\_\_\_  
Office Held

\_\_\_\_\_  
Date