

equipment ("CPE"), call answering, voice mail or messaging, voice storage and retrieval services, fax store and forward, and protocol conversion.

- f. **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.*
- g. **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:

- a. 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.
- b. If the Company employee can use CPNI to assist the customer without disclosing such CPNI to the customer during the call, the employee must: (i) provide the customer with the oral notice set forth in Attachment 3; and (ii) obtain the customer's oral consent to the use of his or her CPNI during the call.

4. **CPNI Not Used for Company-Initiated (Out-Bound) Marketing Purposes.** The Company has adopted a policy that it does not and will not use, disclose, or permit 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). This means that Company employees and agents (as well as the

Company's independent contractors and joint venture partners) are strictly prohibited from accessing or using CPNI to market such services, and from disclosing or distributing CPNI to other employees or agents or outside marketing firms for use in such marketing activities.

NOTE: As detailed in Section D.1 above, this policy does not preclude or restrict the Company from conducting general marketing campaigns (including mass mailings, bill inserts, and telemarketing) to its own customers or to the public at large if CPNI is not used to design such campaigns or target particular customers.

5. **CPNI Not Shared With Affiliates.** The Company has adopted a policy that the CPNI derived from the Company's telecommunications services may not 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 in part by the Company or by the owners of the Company). This means that Company employees are strictly prohibited from disclosing or distributing CPNI to an Affiliate or its employees or agents, and from permitting employees or agents of an Affiliate to access or use records or files containing the Company's CPNI. This also means that 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.

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, the Company's CPNI Compliance Officer must

expressly approve any access, use, disclosure or distribution of CPNI pursuant to this Section E.2 in advance and in writing.

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.

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. An Officer of the Company as an agent of the Company must sign the annual Section 64.2009(e) certification. 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. A separate statement explaining how the Company's operating procedures ensure that it is in compliance with the FCC's CPNI Rules must accompany the certification.
 - 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 4.
2. **Section 64.2009(c) Marketing Record.** The Compliance Officer will maintain a record of each out-bound marketing activity or campaign, 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 at <http://www.fcc.gov/eb/cpni>.
 - 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. The Company must retain each such record 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 pretexter. 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. The ways that the James Garner character on the old "Rockford Files" television series hoodwinked telephone company employees into giving him information were charming and humorous back then. Today, falling for his ruses could get the Company embroiled in an FCC proceeding where it has the burden of proving that it should not be fined \$100,000 or more. 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 telephone 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

Section 222 of The Communications Act

TITLE 47 CHAPTER 5 SUBCHAPTER II Part I § 222

§ 222. Privacy of customer information

(a) In general

Every telecommunications carrier has a duty to protect the confidentiality of proprietary information of, and relating to, other telecommunication carriers, equipment manufacturers, and customers, including telecommunication carriers reselling telecommunications services provided by a telecommunications carrier.

(b) Confidentiality of carrier information

A telecommunications carrier that receives or obtains proprietary information from another carrier for purposes of providing any telecommunications service shall use such information only for such purpose, and shall not use such information for its own marketing efforts.

(c) Confidentiality of customer proprietary network information

(1) Privacy requirements for telecommunications carriers

Except as required by law or with the approval of the customer, a telecommunications carrier that receives or obtains customer proprietary network information by virtue of its provision of a telecommunications service shall only use, disclose, or permit access to individually identifiable customer proprietary network information in its provision of (A) the telecommunications service from which such information is derived, or (B) services necessary to, or used in, the provision of such telecommunications service, including the publishing of directories.

(2) Disclosure on request by customers

A telecommunications carrier shall disclose customer proprietary network information, upon affirmative written request by the customer, to any person designated by the customer.

(3) Aggregate customer information

A telecommunications carrier that receives or obtains customer proprietary network information by virtue of its provision of a telecommunications service may use, disclose, or permit access to aggregate customer information other than for the purposes described in paragraph (1). A local exchange carrier may use, disclose, or permit access to aggregate customer information other than for purposes described in paragraph (1) only if it provides such aggregate information to other carriers or persons on reasonable and nondiscriminatory terms and conditions upon reasonable request therefore.

(d) Exceptions

Nothing in this section prohibits a telecommunications carrier from using, disclosing, or permitting access to customer proprietary network information obtained from its customers, either directly or indirectly through its agents—

- (1) To initiate, render, bill, and collect for telecommunications services;
- (2) To protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services;
- (3) To provide any inbound telemarketing, referral, or administrative services to the customer for the duration of the call, if such call was initiated by the customer and the customer approves of the use of such information to provide such service; and
- (4) To provide call location information concerning the user of a commercial mobile service (as such term is defined in section 332 (d) of this title)—
 - (A) To a public safety answering point, emergency medical service provider or emergency dispatch provider, public safety, fire service, or law enforcement official, or hospital emergency or trauma care facility, in order to respond to the user's call for emergency services;
 - (B) To inform the user's legal guardian or members of the user's immediate family of the user's location in an emergency situation that involves the risk of death or serious physical harm; or
 - (C) To providers of information or database management services solely for purposes of assisting in the delivery of emergency services in response to an emergency.

(e) Subscriber list information

Notwithstanding subsections (b), (c), and (d) of this section, a telecommunications carrier that provides telephone exchange service shall provide subscriber list information gathered in its capacity as a provider of such service on a timely and unbundled basis, under nondiscriminatory and reasonable rates, terms, and conditions, to any person upon request for the purpose of publishing directories in any format.

(f) Authority to use wireless location information

For purposes of subsection (c)(1) of this section, without the express prior authorization of the customer, a customer shall not be considered to have approved the use or disclosure of or access to—

- (1) Call location information concerning the user of a commercial mobile service (as such term is defined in section 332 (d) of this title), other than in accordance with subsection (d)(4) of this section; or
- (2) Automatic crash notification information to any person other than for use in the operation of an automatic crash notification system.

(g) Subscriber listed and unlisted information for emergency services

Notwithstanding subsections (b), (c), and (d) of this section, a telecommunications carrier that provides telephone exchange service shall provide information described in subsection (i)(3)(A) of this section (including information pertaining to subscribers whose information is unlisted or unpublished) that is in its possession

or control (including information pertaining to subscribers of other carriers) on a timely and unbundled basis, under nondiscriminatory and reasonable rates, terms, and conditions to providers of emergency services, and providers of emergency *support services, solely for purposes of delivering or assisting in the delivery of emergency services.*

(h) Definitions

As used in this section:

(1) Customer proprietary network information

The term "customer proprietary network information" means—

- (A) Information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a 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 such term does not include subscriber list information.

(2) Aggregate information

The term "aggregate customer information" means collective data that relates to a group or category of services or customers, from which individual customer identities and characteristics have been removed.

(3) Subscriber list information

The term "subscriber list information" means any information—

- (A) Identifying the listed names of subscribers of a carrier and such subscribers' telephone numbers, addresses, or primary advertising classifications (as such classifications are assigned at the time of the establishment of such service), or any combination of such listed names, numbers, addresses, or classifications; and
- (B) That the carrier or an affiliate has published caused to be published, or accepted for publication in any directory format.

(4) Public safety answering point

The term "public safety answering point" means a facility that has been designated to receive emergency calls and route them to emergency service personnel.

(5) Emergency services

The term "emergency services" means 9--1--1 emergency services and emergency notification services.

(6) Emergency notification services

The term "emergency notification services" means services that notify the public of an emergency.

(7) Emergency support services

The term "emergency support services" means information or data base management services used in support of emergency services.

[1] So in original. Probably should be subsection "(h)(3)(A)".

Attachment 2

FCC CPNI Rules

Title 47 – Telecommunications

Chapter I – Federal Communications Commission (Continued)

Part 64 miscellaneous rules relating to common carriers

Subpart u customer proprietary network information

Sec. 64.2001 Basis and purpose.

(a) Basis. The rules in this subpart are issued pursuant to the Communications Act of 1934, as amended.

(b) Purpose. The purpose of the rules in this subpart is to implement section 222 of the Communications Act of 1934, as amended, 47 U.S.C. 222.

Sec. 64.2003 Definitions.

(a) Account information. "Account information" is information that is specifically connected to the customer's service relationship with the carrier, including such things as an account number or any component thereof, the telephone number associated with the account, or the bill's amount.

(b) Address of record. An "address of record," whether postal or electronic, is an address that the carrier has associated with the customer's account for at least 30 days.

(c) Affiliate. The term "affiliate" has the same meaning given such term in section 3(1) of the Communications Act of 1934, as amended, 47 U.S.C. 153(1).

(d) Call detail information. Any information that pertains to the transmission of specific telephone calls; including, for outbound calls, the number called, and the time, location, or duration of any call, and, for inbound calls, the number from which the call was placed, and the time, location, or duration of any call.

(e) Communications-related services. The term "communications-related services" means telecommunications services, information services typically provided by telecommunications carriers, and services related to the provision or maintenance of customer premises equipment.

(f) Customer. A customer of a telecommunications carrier is a person or entity to which the telecommunications carrier is currently providing service.

(g) Customer proprietary network information (CPNI). The term "customer proprietary network information (CPNI)" has the same meaning given to such term in section 222(h)(1) of the Communications Act of 1934, as amended, 47 U.S.C. 222(h)(1).

(h) Customer premises equipment (CPE). The term "customer premises equipment (CPE)" has the same meaning given to such term in section 3(14) of the Communications Act of 1934, as amended, 47 U.S.C. 153(14).

(i) Information services typically provided by telecommunications carriers. The phrase "information services typically provided by telecommunications carriers" means only those information services (as defined in section 3(20) of the Communication Act of 1934, as amended, 47 U.S.C. 153(20)) that are typically provided by telecommunications carriers, such as Internet access or voice mail services. Such phrase "information services typically provided by telecommunications carriers," as used in this subpart, shall not include retail consumer services provided using Internet Web sites (such as travel reservation services or mortgage lending services), whether or not such services may otherwise be considered to be information services.

(j) Local exchange carrier (LEC). The term "local exchange carrier (LEC)" has the same meaning given to such term in section 3(26) of the Communications Act of 1934, as amended, 47 U.S.C. 153(26).

(k) Opt-in approval. The term "opt-in approval" refers to a method for obtaining customer consent to use, disclose, or permit access to the customer's CPNI. This approval method requires that the carrier obtain from the customer affirmative, express consent allowing the requested CPNI usage, disclosure, or access after the customer is provided appropriate notification of the carrier's request consistent with the requirements set forth in this subpart.

(l) Opt-out approval. The term "opt-out approval" refers to a method for obtaining customer consent to use, disclose, or permit access to the customer's CPNI. Under this approval method, a customer is deemed to have consented to the use, disclosure, or access to the customer's CPNI if the customer has failed to object thereto within the waiting period described in Sec. 64.2008(d)(1) after the customer is provided appropriate notification of the carrier's request for consent consistent with the rules in this subpart.

(m) Readily available biographical information. "Readily available biographical information" is information drawn from the customer's life history and includes such things as the customer's social security number, or the last four digits of that number; mother's maiden name; home address; or date of birth.

(n) Subscriber list information (SLI). The term "subscriber list information (SLI)" has the same meaning given to such term in section 222(h)(3) of the Communications Act of 1934, as amended, 47 U.S.C. 222(h)(3).

(o) Telecommunications carrier or carrier. The terms "telecommunications carrier" or "carrier" shall have the same meaning as set forth in section 3(44) of the Communications

Act of 1934, as amended, 47 U.S.C. 153(44). For the purposes of this subpart, the term "telecommunications carrier" or "carrier" shall include an entity that provides interconnected VoIP service, as that term is defined in section 9.3 of these rules.

(p) Telecommunications service. The term "telecommunications service" has the same meaning given to such term in section 3(46) of the Communications Act of 1934, as amended, 47 U.S.C. 153(46).

(q) Telephone number of record. The telephone number associated with the underlying service, not the telephone number supplied as a customer's "contact information."

(r) Valid photo ID. A "valid photo ID" is a government-issued means of personal identification with a photograph such as a driver's license, passport, or comparable ID that is not expired.

[72 FR 31961, June 8, 2007]

Effective Date Note: At 72 FR 31961, June 8, 2007, Sec. 64.2003 was revised. Paragraphs (a), (b), (d), (m), (o), (q), and (r) of newly revised Sec. 64.2003 contain information collection and recordkeeping requirements and will not become effective until the Office of Management and Budget (OMB) have given approval.

Sec. 64.2005 Use of customer proprietary network information without customer approval.

(a) Any telecommunications carrier may use, disclose, or permit access to CPNI for the purpose of providing or marketing service offerings among the categories of service (i.e., local, interexchange, and CMRS) to which the customer already subscribes from the same carrier, without customer approval.

(1) If a telecommunications carrier provides different categories of service, and a customer subscribes to more than one category of service offered by the carrier, the carrier is permitted to share CPNI among the carrier's affiliated entities that provide a service offering to the customer.

(2) If a telecommunications carrier provides different categories of service, but a customer does not subscribe to more than one offering by the carrier, the carrier is not permitted to share CPNI with its affiliates, except as provided in Sec. 64.2007(b).

(b) A telecommunications carrier may not use, disclose, or permit access to CPNI to market to a customer service offerings that are within a category of service to which the subscriber does not already subscribe from that carrier, unless that carrier has customer approval to do so, except as described in paragraph (c) of this section.

(1) A wireless provider may use, disclose, or permit access to CPNI derived from its provision of CMRS, without customer approval, for the provision of CPE and information

service(s). A wire line carrier may use, disclose or permit access to CPNI derived from its provision of local exchange service or interexchange service, without customer approval, for the provision of CPE and call answering, voice mail or messaging, voice storage and retrieval services, fax store and forward, and protocol conversion.

(2) A telecommunications carrier may not use, disclose or permit access to CPNI to identify or track customers that call competing service providers. For example, a local exchange carrier may not use local service CPNI to track all customers that call local service competitors.

(c) A telecommunications carrier may use, disclose, or permit access to CPNI, without customer approval, as described in this paragraph (c).

(1) A telecommunications carrier may use, disclose, or permit access to CPNI, without customer approval, in its provision of inside wiring installation, maintenance, and repair services.

(2) CMRS providers may use, disclose, or permit access to CPNI for the purpose of conducting research on the health effects of CMRS.

(3) LECs, CMRS providers, and entities that provide interconnected VoIP service as that term is defined in Sec. 9.3 of this chapter, may use CPNI, without customer approval, to market services formerly known as adjunct-to-basic services, such as, but not limited to, speed dialing, computer-provided directory assistance, call monitoring, call tracing, call blocking, call return, repeat dialing, call tracking, call waiting, caller I.D., call forwarding, and certain Centrex features.

(d) A telecommunications carrier may use, disclose, or permit access to CPNI to protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services.

[63 FR 20338, Apr. 24, 1998, as amended at 64 FR 53264, Oct. 1, 1999; 67 FR 59211, Sept. 20, 2002; 72 FR 31962, June 8, 2007]

Effective Date Note: At 72 FR 31962, June 8, 2007, Sec. 64.2005 was amended by revising paragraph (c)(3). This text contains information collection and recordkeeping requirements and will not become effective until the Office of Management and Budget (OMB) have given approval.

Sec. 64.2007 Approval required for use of customer proprietary network information.

(a) A telecommunications carrier may obtain approval through written, oral or electronic methods.

(1) A telecommunications carrier relying on oral approval shall bear the burden of demonstrating that such approval has been given in compliance with the Commission's rules in this part.

(2) Approval or disapproval to use, disclose, or permit access to a customer's CPNI obtained by a telecommunications carrier must remain in effect until the customer revokes or limits such approval or disapproval.

(3) A telecommunications carrier must maintain records of approval, whether oral, written or electronic, for at least one year.

(b) Use of Opt-Out and Opt-In Approval Processes. A telecommunications carrier may, subject to opt-out approval or opt-in approval, use its customer's individually identifiable CPNI for the purpose of marketing communications-related services to that customer. A telecommunications carrier may, subject to opt-out approval or opt-in approval, disclose its customer's individually identifiable CPNI, for the purpose of marketing communications-related services to that customer, to its agents and its affiliates that provide communications-related services. A telecommunications carrier may also permit such persons or entities to obtain access to such CPNI for such purposes. Except for use and disclosure of CPNI that is permitted without customer approval under section Sec. 64.2005, or that is described in this paragraph, or as otherwise provided in section 222 of the Communications Act of 1934, as amended, a telecommunications carrier may only use, disclose, or permit access to its customer's individually identifiable CPNI subject to opt-in approval.

[67 FR 59212, Sept. 20, 2002, as amended at 71 FR 31962, June 8, 2007]

Effective Date Note: At 72 FR 31962, June 8, 2007, Sec. 64.2007 was amended by revising paragraph (b). This text contains information collection and recordkeeping requirements and will not become effective until the Office of Management and Budget (OMB) have given approval.

Sec. 64.2008 Notice required for use of customer proprietary network information.

(a) Notification, Generally. (1) Prior to any solicitation for customer approval, a telecommunications carrier must provide notification to the customer of the customer's right to restrict use of, disclosure of, and access to that customer's CPNI.

(2) A telecommunications carrier must maintain records of notification, whether oral, written or electronic, for at least one year.

(b) Individual notice to customers must be provided when soliciting approval to use, disclose, or permit access to customers' CPNI.

(c) Content of Notice. Customer notification must provide sufficient information to enable the customer to make an informed decision as to whether to permit a carrier to use, disclose, or permit access to, the customer's CPNI.

(1) *The notification must state that the customer has a right, and the carrier has a duty, under federal law, to protect the confidentiality of CPNI.*

(2) The notification must specify the types of information that constitute CPNI and the specific entities that will receive the CPNI, describe the purposes for which CPNI will be used, and inform the customer of his or her right to disapprove those uses, and deny or withdraw access to CPNI at any time.

(3) The notification must advise the customer of the precise steps the customer must take in order to grant or deny access to CPNI, and must clearly state that a denial of approval will not affect the provision of any services to which the customer subscribes. However, carriers may provide a brief statement, in clear and neutral language, describing consequences directly resulting from the lack of access to CPNI.

(4) The notification must be comprehensible and must not be misleading.

(5) If written notification is provided, the notice must be clearly legible, use sufficiently large type, and be placed in an area so as to be readily apparent to a customer.

(6) If any portion of a notification is translated into another language, then all portions of the notification must be translated into that language.

(7) A carrier may state in the notification that the customer's approval to use CPNI may enhance the carrier's ability to offer products and services tailored to the customer's needs. A carrier also may state in the notification that it may be compelled to disclose CPNI to any person upon affirmative written request by the customer.

(8) A carrier may not include in the notification any statement attempting to encourage a customer to freeze third-party access to CPNI.

(9) The notification must state that any approval, or denial of approval for the use of CPNI outside of the service to which the customer already subscribes from that carrier is valid until the customer affirmatively revokes or limits such approval or denial.

(10) A telecommunications carrier's solicitation for approval must be proximate to the notification of a customer's CPNI rights.

(d) Notice Requirements Specific to Opt-Out. A telecommunications carrier must provide notification to obtain opt-out approval through electronic or written methods, but not by oral communication (except as provided in paragraph (f) of this section). The contents of any such notification must comply with the requirements of paragraph (c) of this section.

(1) Carriers must wait a 30-day minimum period of time after giving customers notice and an opportunity to opt-out before assuming customer approval to use, disclose, or permit access to CPNI. A carrier may, in its discretion, provide for a longer period. Carriers *must notify customers as to the applicable waiting period for a response before approval is assumed.*

(i) In the case of an electronic form of notification, the waiting period shall begin to run from the date on which the notification was sent; and

(ii) In the case of notification by mail, the waiting period shall begin to run on the third day following the date that the notification was mailed.

(2) Carriers using the opt-out mechanism must provide notices to their customers every two years.

(3) Telecommunications carriers that use e-mail to provide opt-out notices must comply with the following requirements in addition to the requirements generally applicable to notification:

(i) Carriers must obtain express, verifiable, prior approval from consumers to send notices via e-mail regarding their service in general, or CPNI in particular;

(ii) Carriers must allow customers to reply directly to e-mails containing CPNI notices in order to opt-out;

(iii) Opt-out e-mail notices that are returned to the carrier as undeliverable must be sent to the customer in another form before carriers may consider the customer to have received notice;

(iv) Carriers that use e-mail to send CPNI notices must ensure that the subject line of the message clearly and accurately identifies the subject matter of the e-mail; and

(v) Telecommunications carriers must make available to every customer a method to opt-out that is of no additional cost to the customer and that is available 24 hours a day, seven days a week. Carriers may satisfy this requirement through a combination of methods, so long as all customers have the ability to opt-out at no cost and are able to effectuate that choice whenever they choose.

(e) Notice Requirements Specific to Opt-In. A telecommunications carrier may provide notification to obtain opt-in approval through oral, written, or electronic methods. The contents of any such notification must comply with the requirements of paragraph (c) of this section.

(f) Notice Requirements Specific to One-Time Use of CPNI. (1) Carriers may use oral notice to obtain limited, one-time use of CPNI for inbound and outbound customer

telephone contacts for the duration of the call, regardless of whether carriers use opt-out or opt-in approval based on the nature of the contact.

(2) The contents of any such notification must comply with the requirements of paragraph (c) of this section, except that telecommunications carriers may omit any of the following notice provisions if not relevant to the limited use for which the carrier seeks CPNI:

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

(ii) Carriers need not advise customers that they may share CPNI with their 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) Carriers need not disclose the means by which a customer can deny or withdraw future access to CPNI, so long as carriers explain to customers that the scope of the approval the carrier seeks is limited to one-time use; and

(iv) Carriers may omit disclosure of the precise steps a customer must take in order to grant or deny access to CPNI, as long as the carrier clearly communicates that the customer can deny access to his CPNI for the call.

[67 FR 59212, Sept. 20, 2002]

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

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

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

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

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

(e) A telecommunications carrier must have an officer, as an agent of the carrier, sign and file with the Commission a compliance certificate on an annual basis. The officer must state in the certification that he or she has personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the rules in this subpart. The carrier must provide a statement accompanying the certificate explaining how its operating procedures ensure that it is or is not in compliance with the rules in this subpart. In addition, the carrier must include an explanation of any actions taken against data brokers and a summary of all customer complaints received in the past year concerning the unauthorized release of CPNI. This filing must be made annually with the Enforcement Bureau on or before March 1 in EB Docket No. 06-36, for data pertaining to the previous calendar year.

(f) Carriers must provide written notice within five business days to the Commission of any instance where the opt-out mechanisms do not work properly, to such a degree that consumers' inability to opt-out is more than an anomaly.

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

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

[63 FR 20338, Apr. 24, 1998, as amended at 64 FR 53264, Oct. 1, 1999; 67 FR 59213, Sept. 20, 2002; 72 FR 31962, June 8, 2007]

Effective Date Note: At 72 FR 31962, June 8, 2007, Sec. 64.2009 was amended by revising paragraph (e). This text contains information collection and recordkeeping requirements and will not become effective until the Office of Management and Budget (OMB) have given approval.

Attachment 3

Sample Written 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 4

Sample CPNI Compliance Certificate
[Section 64.2009(e) of FCC Rules]

EB DOCKET NO. 06-36

I, Frank D. Richter, hereby certify that I am an Officer of Western Independent Networks, Inc. (WIN), and am executing this CPNI Compliance Certificate as its agent.

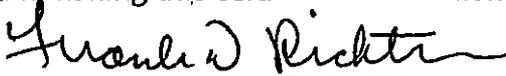
I have personal knowledge that WIN has established operating procedures that are adequate to ensure compliance with the Customer Proprietary Network Information rules and requirements in Subpart U of Part 64 of the Federal Communications Commission's Rules (47 C.F.R. §§64.2001 through 64.2011).

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 2008.



Signature

Frank D. Richter _____
Printed Name

President _____
Office Held

02-04-09 _____
Date

Western Independent Networks

**STATEMENT EXPLAINING HOW THE COMPANY'S OPERATING PROCEDURES
ENSURE COMPLIANCE WITH THE FCC'S CPNI RULES**

I. Customer Proprietary Network Information ("CPNI")

CPNI is defined in Section 222(f) 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 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 telecommunications services. CPNI encompasses information such as: (a) the telephone numbers called by a consumer; (b) the telephone numbers calling a customer; (c) the time, location and duration of a consumer's outbound and inbound phone calls, and (d) the telecommunications and information services purchased by a consumer.

Call detail information (also known as "call records") is a category of CPNI that is particularly sensitive from a privacy standpoint and that is sought by pretexters, hackers and other unauthorized entities for illegitimate purposes. Call detail includes any information that pertains to the transmission of a specific telephone call, including the number called (for outbound calls), the number from which the call was placed (for inbound calls), and the date, time, location and/or duration of the call (for all calls).

II. Use and Disclosure of CPNI Is Restricted

WIN recognizes that CPNI includes information that is personal and individually identifiable, and that 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.

WIN 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.

WIN employees and agents that may deal with CPNI have been informed that there are substantial federal restrictions upon CPNI use, distribution and access. In order to be authorized to use or access WIN's CPNI, employees and agents must receive training with respect to the requirements of Section 222 of the Communications Act and the FCC's CPNI Rules (Subpart U of Part 64 of the FCC Rules).

Before an agent, independent contractor or joint venture partner may receive or be allowed to access or use WIN's CPNI, the agent's, independent contractor's or joint venture partner's agreement with WIN 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.

III. Protection of CPNI

1. WIN may, after receiving an appropriate written request from a customer, disclose or provide the customer's CPNI to the customer by sending it to the customer's address of record. 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 must be disclosed or provided; (4) must specify the time period for which the CPNI must be disclosed or provided; and (5) must be signed by the customer. The Company will disclose CPNI upon affirmative written request by the customer to any person designated by the customer, but only after WIN calls the customer's telephone number of record and/or sends a notification to the customer's address of record to verify the accuracy of this request.
2. WIN will provide a customer's phone records or other CPNI to a law enforcement agency in accordance with applicable legal requirements.
3. WIN will retain all customer passwords and "shared secret" question-answer combinations in secure files that may be accessed only by authorized WIN employees who need such information in order to authenticate the identity of customers requesting call detail information over the telephone.
4. WIN employees will authenticate all telephone requests for CPNI in the same manner whether or not the CPNI consists of call detail information. That is, WIN employees must: (a) be furnished the customer's pre-established password (or correct answers to the 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.
5. WIN has adopted a policy that it does not and will not use, disclose or permit access to CPNI by an affiliate.
 6. When an existing customer calls WIN to inquire about or order new, additional or modified services (in-bound marketing), WIN may use the customer’s CPNI other than call detail CPNI to assist the customer for the duration of the customer’s call if the Company provides the customer with the oral notice required by Sections 64.2008(c) and 64.2008(f) of the FCC’s Rules and after WIN authenticates the customer.
 7. WIN may disclose or release call detail information to customers during customer-initiated telephone contacts only when the customer provides a pre-established password. If the customer does not provide a password, call detail information can be released only by sending it to the customer’s address of record or by the carrier calling the customer at the telephone number of record. If the customer is able to provide to WIN during a customer-initiated telephone call, all of the call detail information necessary to address a customer service issue (*i.e.*, the telephone number called, when it was called, and, if applicable, the amount charged for the call) without WIN assistance, then WIN may take routine customer service actions related to such information. (However, under this circumstance, WIN may not disclose to the customer any call detail information about the customer account other than the call detail information that the customer provides without the customer first providing a password.)
 8. WIN 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 Out-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.
 9. Before a customer’s CPNI can be used in an out-bound marketing activity or campaign, WIN’s records must be checked to determine the status of the customer’s CPNI approval. WIN employees, 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.

If new, additional or extended approvals are necessary; the CPNI Compliance Officer will determine whether the Company’s “Opt-Out CPNI Notice” or “Opt-In CPNI Notice” must be used with respect to various proposed out-bound marketing activities.

10. 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 one year.
11. WIN's employees may use CPNI to initiate, render, bill and collect for telecommunications services. WIN 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, WIN's employees 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.
12. WIN's employees may use CPNI without customer approval to protect WIN'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.

Because allegations and investigations of fraud, abuse and illegal use constitute very sensitive matters, WIN's CPNI Compliance Officer must expressly approve any access, use, disclosure or distribution of CPNI pursuant to this Section in advance and in writing.
13. WIN'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. Nor may WIN's employees, agents, independent contractors or joint venture partners' use or disclose CPNI for personal reasons or profit.
14. Company policy mandates that files containing CPNI be maintained in a secure manner such that they cannot be used, accessed, disclosed or distributed by unauthorized individuals or in an unauthorized manner.
15. Paper files containing CPNI are kept in secure areas, and may not be used, removed, or copied in an unauthorized manner.
16. Electronic files and databases containing CPNI are maintained on computers that are not accessible from the Internet. Electronic files and databases may be accessed only by authorized WIN employees who have been provided a currently effective strong login ID and password (which password is periodically changed).

17. WIN employees, agents, independent contractors and joint venture partners are required to notify the CPNI Compliance Officer of any access or security problems they encounter with respect to files containing CPNI.

18. Customers may obtain an initial or replacement password: (i) if they come in person to WIN'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 WIN telephone number from their telephone number of record, and then wait at that number until a WIN representative calls them back and obtains correct answers to certain questions regarding their service and address.

19. WIN 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: (a) change or request for change of the customer's password; (b) change or request for change of the customer's address of record; and (c) 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: (a) a Company call or voicemail to the customer's telephone number of record; or (b) 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.

 - d. WIN employee or agent sending the notice must prepare and furnish to the CPNI Compliance Officer a memorandum containing: (a) the name, address of record, and telephone number of record of the customer notified; (b) a copy or the exact wording of the written notice, telephone message or voicemail message comprising the notice; and (c) the date and time that the notice was sent.

20. WIN 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 WIN discovers that a person (without authorization or exceeding authorization) has intentionally gained access to, used or disclosed CPNI, WIN 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 at <http://www.fcc.gov/eb/cpni>.

21. WIN will provide customers with access to CPNI at are location if the customer presents a valid photo ID and the valid photo ID matches the name on the account.
22. WIN takes reasonable measures to discover and protect against activity that is indicative of pretexting including requiring WIN employees, agents, independent contractors and joint venture partners 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 WIN'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.

IV. CPNI Compliance Officer

In addition to the specific matters required to be reviewed and approved by WIN's CPNI Compliance Officer, employees and 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 WIN'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 received appropriate guidance is a material consideration in any disciplinary action brought against the employee or agent for impermissible use, disclosure or access to CPNI.

V. Disciplinary Procedures

WIN has informed its employees and agents, independent contractors and joint venture partners that it considers compliance with the Communications Act and FCC Rules regarding the use, disclosure, and access to CPNI to be very important. Violation by WIN employees or agents of such CPNI requirements will lead to disciplinary action (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 WIN independent contractors or joint venture partners of such CPNI requirements will lead to prompt disciplinary action (up to and including remedial training and termination of the contract).

Western Independent Networks

STATEMENT OF ACTIONS TAKEN AGAINST DATA BROKERS

A. During Calendar Year 2008, the Company has instituted the following proceeding, or filed the following petitions, against data brokers before the Federal Communications Commission:

NONE

B. During Calendar Year 2008, the Company has instituted the following proceeding, or filed the following petitions, against data brokers before the Oregon Public Utility Commission:

NONE

C. During Calendar Year 2008, the Company has instituted the following proceeding, or filed the following petitions, against data brokers before the [NAME OF COURT]:

NONE

Western Independent Networks

**SUMMARY OF CUSTOMER COMPLAINTS
REGARDING UNAUTHORIZED RELEASE OF CPNI**

A. During Calendar Year 2008, the Company has received the following number of customer complaints related to unauthorized access to, or disclosure of, CPNI due to improper access by Company employees:

NONE

B. During Calendar Year 2008, the Company has received the following number of customer complaints related to unauthorized access to, or disclosure of, CPNI due to improper disclosure to individuals not authorized to receive the information:

NONE

C. During Calendar Year 2008, the Company has received the following number of customer complaints related to unauthorized access to, or disclosure of, CPNI due to improper access to online information by individuals not authorized to view the information:

NONE

D. During Calendar Year 2008, the Company has become aware of the following processes that pretexters are using to attempt to access its CPNI:

NONE

Attachment 5

CPNI Policy Acknowledgement

I hereby state and acknowledge that I have received a copy of the **CUSTOMER PROPRIETARY NETWORK INFORMATION COMPLIANCE MANUAL** (December 2008 Version), that I am responsible for reviewing and understanding this Manual, that I have attended a training session pertaining to the subjects covered in this Manual, and that I understand that any violation of the Company's CPNI procedures may result in disciplinary action up to and including dismissal.

Frank D Richter
Signature

2/4/09
Date

Frank. D Richter
Print name

WITNESSED:

CPNI COMPLIANCE OFFICER

April L. McClure
Signature

2/4/09
Date

April L. McClure
Print name