

Annual 47 C.F.R. § 64.2009(e) CPNI Certification

Annual 64.2009(e) CPNI Certification for 2016 covering the prior calendar year 2015

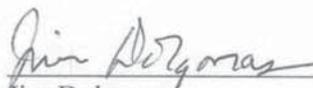
1. Date filed: February 26, 2016
2. Name of company covered by this certification: CENIC Broadband Initiatives, LLC
3. Form 499 Filer ID: 829111
4. Name of signatory: Jim Dolgonas
5. Title of signatory: Manager
6. Certification:

I, Jim Dolgonas, certify that I am an officer of CENIC Broadband Initiatives, LLC (“CBI”) and, acting as its agent, certify that I have personal knowledge that the company has established operating procedures, as summarized in the attached statement, that are adequate to ensure compliance with the customer proprietary network information (“CPNI”) rules as set forth in Part 64, Subpart U of the Commission’s rules, 47 C.F.R. §§ 64.2001 *et seq.*

Attached to this certification is an accompanying statement explaining how CBI’s procedures ensure that it is in compliance with the requirements (including those mandating the adoption of CPNI procedures, training, recordkeeping, and supervisory review) set forth in section 64.2001 *et seq.* of the Commission’s rules.

CBI has not received any customer complaints in the past calendar year concerning unauthorized release of CPNI. CBI has therefore not taken any actions in the past year against data brokers, including proceedings instituted or petitions filed by the company at either state commissions, the court system or at the Commission.

I hereby represent and warrant that the above certification is consistent with Section 1.17 of the Commission’s rules, 47 C.F.R. § 1.17, which requires truthful and accurate statements to the Commission, and acknowledge that false statements and misrepresentations to the Commission are punishable under Title 18 of the U.S. Code and may subject CBI to enforcement actions.



Jim Dolgonas
Manager
CENIC Broadband Initiatives, LLC
Executed February 24, 2016

CENIC Broadband Initiatives (CBI)

CPNI Compliance Policies

The following summary describes the policies of CENIC Broadband Initiatives, LLC (“CBI”) that are designed to protect the confidentiality of Customer Proprietary Network Information (“CPNI”) and to assure compliance with the rules of the Federal Communications Commission (“FCC”) set forth in 47 C.F.R. Part 64, Subpart U, Section 2001 *et seq.* CPNI is “(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.”

This policy does not apply to CBI’s practices with respect to CPNI associated with any broadband Internet access services, which became subject to the requirements of Section 222 of the Communications Act effective June 12, 2015, but which are not subject to the FCC’s CPNI rules. CBI is committed to engaging in reasonable, good-faith steps to protect broadband CPNI from unauthorized use or disclosure.

I. USE, DISCLOSURE OF, AND ACCESS TO CPNI

CBI will use, disclose, or permit access to individually identifiable CPNI only in its provision of the communications service from which such information is derived; for services necessary to, or used in, the provision of such communications service, including the publishing of directories; to initiate, render, bill and collect for communications services; to protect the rights or property of CBI or to protect users or other carriers or service providers from fraudulent, abusive or unlawful use of, or subscription to, such services; to provide inside wiring installation, maintenance, or repair services; as required by law; or as expressly authorized by the customer.

CBI does not use CPNI to market service offerings among the different categories of service, or even within the same category of service, that it provides to subscribers. Although CBI’s current policy is not to use CPNI for marketing, in the event that any employee or agent wishes to use CPNI for marketing or to seek customer approval for such use, such proposed use is subject to a supervisory review process that shall involve the CPNI Compliance Manager. If such use is approved, CBI shall modify these policies and conduct additional training as needed to assure compliance with the FCC’s rules.

CBI does not use, disclose or permit access to CPNI to identify or track customers that contact competing service providers.

When CBI receives or obtains proprietary information from another carrier for purposes of providing a telecommunications service, it shall use such information only for such purpose, and not for its own marketing efforts.

II. SAFEGUARDS AGAINST DISCLOSURE OF CPNI TO UNAUTHORIZED PARTIES

Above and beyond the specific FCC requirements, CBI will take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI. If any employee becomes aware of new methods that are being used or could be used by third parties to attempt to obtain unauthorized access to CPNI, or of possible changes to CBI's existing policies that would strengthen protection of CPNI, they should report such information immediately to the CPNI Compliance Manager so that CBI may evaluate whether existing policies should be supplemented or changed.

A. Inbound Calls to CBI Requesting CPNI

CSRs may not disclose any CPNI to an inbound caller until the caller's identity has been authenticated.

Notwithstanding the foregoing, CBI does not provide to inbound callers any Call Detail Information (CDI), which includes 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.

B. In-Person Disclosure of CPNI

CBI does not disclose CPNI to persons at company offices.

C. Online Accounts

Unique usernames and passwords for access to the online portal are created for the customer at the time of the initial service deployment. The password will not consist of Customer's account or biographical information, or easily guessed information.

D. Notice of Account Changes

Whenever a password or online account is created or changed, CBI will provide a notice to a customer address of record. Whenever a postal or e-mail address of record is created or changed, CBI will send a notice to customer's prior address of record notifying them of the change. The foregoing notifications are not required when the customer initiates service, including the selection of an email address or creation of an online account at service initiation.

Each of the notices provided under this paragraph will not reveal the changed information and will direct the customer to notify CBI if they did not authorize the change.

III. REPORTING CPNI BREACHES TO LAW ENFORCEMENT

Any CBI employee that becomes aware of any breaches, suspected breaches or attempted breaches must report such information immediately to the CPNI Compliance Manager. Such information must not be reported or disclosed by any employee to any non-employee, including

the potentially affected customer, except in express conformance with the procedures described below. Any employee that fails to report such information will be subject to disciplinary action that may include termination.

It is CBI's policy that employees should not be discouraged from reporting information about breaches that may have been caused in part by their own actions or omissions. Once a breach has occurred, the most important objective is to attempt to limit the damage to our customers, make any adjustments as needed to prevent a recurrence of the breach, and to alert law enforcement promptly. Therefore, although employees who violate CBI's CPNI compliance procedures are subject to discipline, the sanctions may be substantially reduced where employees promptly self-report violations if appropriate.

A. Identifying a "Breach"

A "breach" has occurred when a person, without authorization or exceeding authorization, has intentionally gained access to, used, or disclosed CPNI. If an employee has information about an incident and is not certain that the incident would not constitute a breach under this definition, the incident must be reported to the CPNI Compliance Manager.

If a CBI employee determines that an unauthorized person is attempting to gain access to CPNI but does not succeed at doing so, no breach has occurred. However, the incident must be reported to CBI's CPNI Compliance Manager who will determine whether to report the incident to law enforcement and/or take other appropriate action. The CPNI Compliance Manager will determine whether it is appropriate to update CBI's CPNI policies or training materials in light of any new information; the FCC's rules require CBI on an ongoing basis to "take reasonable measures to discover and protect against activity that is indicative of pretexting."

B. Notification Procedures

As soon as practicable, and in no event later than seven (7) business days upon learning of a breach, the CPNI Compliance Manager shall electronically notify the United States Secret Service (USSS) and the Federal Bureau of Investigation (FBI) by accessing the following link: <https://www.cpnireporting.gov>. CBI will not notify customers or otherwise disclose a breach until 7 full business days have passed after notification to the USSS and the FBI, but will delay such notification upon the request of either agency. (A full business day does not count a business day on which the notice was provided.) Federal law requires compliance with this requirement even if state law requires disclosure. If CBI receives no response from law enforcement after the 7th full business day, it must promptly proceed to inform the customers whose CPNI was disclosed of the breach.

IV. RECORD RETENTION

The CPNI Compliance Manager is responsible for assuring that we maintain for at least two years a record, electronically or in some other manner, of any breaches discovered, notifications made to the USSS and the FBI pursuant to these procedures, and notifications of breaches made

to customers. The record must include, if available, dates of discovery and notification, a detailed description of the CPNI that was the subject of the breach, and the circumstances of the breach.

CBI maintains a record, for a period of at least one year, of those limited circumstances in which CPNI is disclosed or provided to third parties or where third parties were allowed access to CPNI. If CBI later changes its policies to permit the use of CPNI for marketing, it will revise its recordkeeping policies to comply with the Commission's recordkeeping requirements.

CBI maintains a record of all customer complaints related to their handling of CPNI, and records of CBI's handling of such complaints, for at least two years. The CPNI Compliance Manager will assure that all complaints are reviewed and that CBI considers any necessary changes to its policies or practices to address the concerns raised by such complaints.

V. TRAINING

All employees with access to CPNI receive a copy of CBI's CPNI policies and are informed that (i) any use or disclosure of CPNI or other act or omission not in compliance with such policies will result in disciplinary action, including the termination of employment where appropriate, and (ii) employees who knowingly facilitate the unauthorized disclosure of a customer's confidential information may be subject to criminal penalties. In addition, CBI requires CPNI training for all CSRs, personnel at retail offices that may receive requests for CPNI, and marketing personnel.