

Annual 47 C.F.R. § 64.2009(e)
CPNI Certification Template (EB Docket 06-36)

Annual 64.2009(e) CPNI Certification for 2013 covering the prior calendar year 2012

Name of company(s) covered by this certification: 7seas Connect, LLC

Form 499 Filer ID: 828017

Name of signatory: Amer Almoalem

Title of signatory: President

I, Amer Almoalem, certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. See 47 C.F.R. § 64.2001 *et seq.*

Attached to this certification is an accompanying statement explaining how the company's procedures ensure that the company 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.

The company agrees to abide by the FCC's CPNI rules as outline in the attached statement ("Statement of CPNI Procedures and Compliance").

The company HAS NOT taken actions (*i.e.*, proceedings instituted or petitions filed by a company at either state commissions, the court system, or at the Commission against data brokers) against data brokers in the past year.

The company HAS NOT received customer complaints in the past year concerning the unauthorized release of CPNI.

The company represents and warrants that the above certification is consistent with 47. C.F.R. § 1.17 which requires truthful and accurate statements to the Commission. The company also acknowledges that false statements and misrepresentations to the Commission are punishable under Title 18 of the U.S. Code and may subject it to enforcement action.

Signed:



Date: February 28, 2013

7seas Connect, LLC

Statement of CPNI Procedures and Compliance

This statement accompanies the Company's 2012 Customer Proprietary Network Information ("CPNI") Certification, as required by Section 64.2009(e) of the Federal Communications Commission's ("FCC's") rules, for the purpose of explaining how the operating procedures of the Company ensure compliance with Part 64, Subpart U of the FCC's rules. See 47 C.F.R. § 64.2001 *et seq.*

All subsequent references to rule Sections refer to the FCC's CPNI rules under 47 C.F.R. § 64.2009, unless indicated otherwise.

Identification of CPNI

The Company has established procedures and trained employees having access to, or occasion to use customer data, to identify what customer information is CPNI consistent with the definition of CPNI the FCC's rules.

Procedures Protecting Against Disclosure of CPNI

The Company has implemented procedures for compliance with the FCC's CPNI rules, including, but not limited to the following:

- The Company provides customers with on-line access to customer account information for which the Company has initiated procedures to control access comprising authentication through a password.
- The Company has implemented password back-up authentication procedures.
- The Company has implemented procedures to notify customers of account changes.
- Authentication of customers before disclosing CPNI on customer-initiated telephone contacts.

The Company does not have any retail locations and therefore does not disclose CPNI in-store.

Identification of Permissible Uses of CPNI without Customer Authorization

The Company has established procedures and trained employees having access to, or occasion to use CPNI, to identify uses of CPNI requiring and not requiring customer authorization under the FCC's rules.

Use of CPNI in Marketing Campaigns

As of this date, the Company does not use or permit access to CPNI to market any telecommunications or non-telecommunications services. The Company has trained its personnel not to use CPNI for marketing purposes. Should the Company elect to use CPNI in future marketing efforts, it will follow the applicable rules set forth in the FCC's CPNI rules, including, if necessary, the institution of operational procedures to ensure that notification is provided and customer approval is obtained before CPNI is used or disclosed.

Customer Notification and Authorization Process

The Company does not use CPNI for marketing and thus, at this time, has not provided notice regarding Opt-Out. Prior to any planned use of CPNI for marketing, the Company will initiate the notification and Opt-Out process. The Company does not provide CPNI to other parties and thus has not used the opt-in approval process. The Company has trained employees regarding prohibitions on use of CPNI for marketing. Prior to initiation of any program for use of CPNI for marketing, the Company will train employees with a need and/or responsibility for obtaining customer authorization to use CPNI for marketing purposes, regarding the notice and approval requirements under Section 64.2008.

Record of Customer CPNI Approval

At such time as Company may initiate use of CPNI for marketing with corresponding launch of a notification and Opt-Out process, the Company will develop and utilize a system for maintaining readily accessible record of whether and how a customer has responded to Opt-Out approval as required by Section 64.2009(a).

Disclosure of CPNI to Third Parties

The Company does not disclose CPNI to any agents, affiliates, joint venture partners or independent contractors, nor does it use CPNI to identify or track customers who call competing providers. The Company has a strict policy prohibiting the disclosure of CPNI to any third parties, unless required to do so by law (e.g., in response to a subpoena).

Disciplinary Process

The Company has in place an express disciplinary process to address any unauthorized use of CPNI where the circumstances indicate authorization is required under Section 64.2009(b).

Supervisory Review Process for Outbound Marketing

Before undertaking to use CPNI for outbound marketing purposes, the Company will establish a supervisory review process to ensure compliance with Section 64.2009(d) of the FCC's rules.

Procedures for Notifying Law Enforcement of CPNI Security Breaches

The Company has procedures in place to notify law enforcement in the event of a breach of customers' CPNI and to ensure that the affected customers are not notified of the breach before the

time period set forth in the FCC's rules, or, if applicable, when so authorized by law enforcement. Specifically, as soon as practicable, and in no case later than seven business days upon learning of a breach, the company will notify the U.S. Secret Service and the FBI by electronic means, as required by FCC regulations. The company will not notify customers or disclose a breach to the public until seven full business days have passed after notification to the

U.S. Secret Service and the FBI, unless it believes there is an extraordinarily urgent need to notify customers before seven days in order to avoid immediate and irreparable harm. In that instance, it will only notify such customers after consultation with the relevant investigating agency and will cooperate with the agency's request to minimize any adverse effects of the customer notification. If the Company receives no response from law enforcement after the seventh full business day, it will promptly proceed to inform the customers whose CPNI was disclosed of the breach. The company will delay notification to customers or the public if requested to do so by the U.S. Secret Service or FBI. Notifications to law enforcement and customers are handled by a designated supervisor level employee responsible for managing the company's CPNI compliance.

Actions Taken Against Data Brokers and Responses to Customer Complaints

Pursuant to Section 64.2009, the Company makes the following 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:

Not applicable. No actions taken against data-brokers.

No customer complaints received.

47 C.F.R. § 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.