Industry Assurance Consulting, Inc.

IAC Advice* – *Compliance, Consulting, Certifications
Telephone: (786) 505-1862
6303 Blue Lagoon Drive, Suite 400, Miami, FL 33126
www.iacadvice.com®, Email: **compliance@iacadvice.com**

January 1, 2019

BY ELECTRONIC SUBMISSION

Marlene H. Dortch, Secretary
Federal Communications Commission
Office of the Secretary
445 12th Street, S.W., Suite TW-A325
Washington, DC 20554

Subject: EB Docket No. 06-36, CPNI Certification due March 1, 2019 (CY 2018 Operations)

Dear Ms. Dortch:

Sit-Co, LLC (*hereby referred to as the "Company"*), submits the following CPNI Certification, regarding its Calendar Year 2018 operations, in compliance with Section 64.2001 et seq. of the Commission's rules.

The Company respectfully asks the Commission to accept the following Certification as timely filed, in terms of the March 1, 2019 filing deadline listed in 47 C.F.R. 64.2009(e).

Alonzo Beyene
Industry Assurance Consulting, Inc.
Regulatory Analyst

Enclosures

cc: FCC Enforcement Bureau, Telecommunications Consumers Division,
445 12th Street, SW, Washington, DC 20554
Best Copy and Printing, Inc. (via email fcc@bcpiweb.com)

EB Docket 06-36

Annual 64.2009(e) CPNI Certification for Activities of Calendar Year **2018**
Date filed: **January 1, 2019**
Name of The Company(s) covered by this certification: **Sit-Co, LLC**
Form 499 Filer ID: **829050**
Name of signatory: **Tom Kolb**
Title of signatory: **Managing Member**

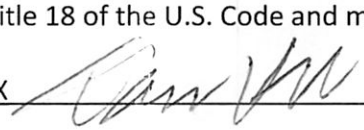
I, **Tom Kolb**, certify that I am an officer of the Company named above, and acting as an agent of the Company, that I have personal knowledge that the Company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. See 47 C.F.R. § 64.2001 *et seq*.

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 **has not had to take any action(s)** (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. If affirmative, the Company is aware that it must explain any actions that it has had to take against data brokers. The Company is aware that it must report on any data that it has with respect to the processes that any pretexters have used (if any), to attempt to access CPNI, and what steps the Company is taking to protect CPNI.

The Company **has not** received any customer complaints in the past year concerning the unauthorized release of CPNI. The Company is aware, that had it had any such complaints, it would have to report the number of customer complaints that the Company has received related to unauthorized access to CPNI, or unauthorized disclosure of CPNI, broken down by category of complaints, e.g., instances of improper access by employees, instances of improper disclosure to individuals not authorized to receive the data, or instances of improper access to online data by individuals not authorized to view the data.

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 X  [*Signature of an officer, as agent of the carrier*]

Attachments: Accompanying Statement explaining CPNI procedures

Accompanying Statement on Company's Compliance with 47 C.F.R. § 64.2009, "Safeguards required for use of Customer Proprietary Network Information (CPNI)" and Compliance with Section 64.2001 et seq. of the Commission's Rules.

A. Definitions

CPNI (*Customer Proprietary Network Data*) refers to data such as customer name, address, contact data as well as quantity, technical configuration, type, destination, and amount of use of service subscribed to by the Company's customers, and made available by the Company's customers to the company, solely by virtue of the customer relationship to the company. It also includes data contained in customer bills, if applicable.

B. Use of CPNI

(1) The Company may, if applicable, 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 Company, without customer approval.

(2) The Company does not use, disclose, or permit access to CPNI to market service offerings to a customer that require opt-in or opt-out consent of a customer under 47 C.F.R. § 64.2001 et seq.

(3) The Company does not use, disclose or permit access to CPNI to identify or track customers that call competing service providers.

(4) Notwithstanding the forgoing: It is the Company's policy that the Company may use, disclose, or permit access to CPNI to protect the rights or property of the Company, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services.

C. Safeguards Required for the Use of CPNI

(1) It is the policy of the Company to train its applicable personnel, on the circumstances under which CPNI may, and may not, be used or disclosed. It is a violation of the Company's policies to disclose CPNI outside of the Company. Any employee that is found to have violated this policy will be subject to disciplinary action up to and including termination.

(2) It is the Company's policy to require that a record be maintained of its own and its affiliates' sales and marketing campaigns that use their customers' CPNI. The Company maintains a record of all instances where CPNI was disclosed or provided to other third-parties, or where third-parties were allowed to access such CPNI. The record includes 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. Such records are retained for a minimum of one year.

(3) The Company has established a mandatory supervisory review process regarding compliance with CPNI rules for outbound marketing. If applicable, sales personnel must obtain supervisory approval of any proposed outbound marketing request for customer approval. The Company's policies require that records pertaining to such carrier compliance be retained for a minimum period of one year.

(4) In compliance with Section 64.2009(e), the Company will prepare a "compliance certificate" signed by an officer on an annual basis stating that the officer has personal knowledge that the Company has established operating procedures that are adequate to ensure compliance with 47 C.F.R. § 64.2001 et seq. The certificate is to be accompanied by this statement and will be filed in EB Docket No. 06-36 annually on March 1, for data pertaining to the previous calendar year. This filing will 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.

D. Safeguards on the Disclosure of CPNI

It is the Company's policy to take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI. The Company will properly authenticate a customer prior to disclosing CPNI based on customer-initiated telephone contact or online access, as described herein.

(1) ***Methods of Accessing CPNI.***

(a) **Telephone Access to CPNI**. It is the Company's policy to only disclose call detail data over the telephone, based on customer-initiated telephone contact, if the customer first provides the Company with a password, as described in Section (2), that is not prompted by the carrier asking for readily available biographical data, or account data. If the customer is able to provide call detail data to the Company during a customer-initiated call without the Company's assistance, then the Company may discuss the call detail data provided by the customer.

(b) **Online Access to CPNI**. It is the Company's policy to authenticate a customer without the use of readily available biographical data, or account data, prior to allowing the customer online access to CPNI related to a telecommunications service account. Once authenticated, the customer may only obtain online access to CPNI related to a telecommunications service account through a password, as described in Section (2), that is not prompted by the Company asking for readily available biographical data, or account data.

(2) ***Password Procedures***
To establish a password, the Company will authenticate the customer without the use of readily available biographical data, or account data. The Company may create a back-up customer authentication method in the event of lost or forgotten passwords, but such back-up customer authentication method will not prompt the customer for readily available biographical data or account data. If the customer cannot provide the correct password or correct response for the back-up customer authentication method, the customer must establish a new password as described in this paragraph.

(3) ***Notification of Account Changes***
The Company will notify customers immediately whenever a password, customer response to a back-up means of authentication for lost or forgotten passwords, online account, or address of record is created or changed. This notification is not required when the customer initiates service, including the selection of a password at service initiation. This notification may be through a Company-originated voicemail or text message to the telephone number of record, or by mail to the address of record, and must not reveal the changed data or be sent to the new account data.

(4) ***Business Customer Exemption***
The Company may bind itself contractually to authentication regimes other than those described in this Section D for services it provides to its business customers that have both a dedicated account representative and a contract that specifically addresses the Company's protection of CPNI.

E. Notification of CPNI Security Breaches
(1) It is the Company's policy to notify law enforcement of a breach in its customers' CPNI as provided in this section. The Company will not notify its customers or disclose the breach publicly until it has completed the process of notifying law enforcement pursuant to paragraph (2).

(2) As soon as practicable, and in no event later than seven (7) business days, after reasonable determination of the breach, the Company will electronically notify the applicable US government agencies such as the Federal Bureau of Investigation.

(a) Notwithstanding state law to the contrary, the Company will not notify customers or disclose the breach to the public until 7 full business days have passed after notification to applicable US government agencies, except as provided in paragraphs (b) and (c).

(b) If the Company believes that there is an extraordinarily urgent need to notify any class of affected customers sooner than otherwise allowed under paragraph (a), in order to avoid immediate and irreparable harm, it will so indicate in its notification and may proceed to immediately notify its affected customers only after consultation with the relevant investigation agency. The Company will cooperate with the relevant investigating agency's request to minimize any adverse effects of such customer notification.

(c) If the relevant investigating agency determines that public disclosure or notice to customer would impede or compromise an ongoing or potential criminal investigation or national security, the Company will comply with such agency's written directives, including directives not to so disclose or notify for an initial period of up to 30 days, and extended periods as reasonably necessary in the judgment of the agency.

(3) After the Company has completed the process of notifying law enforcement pursuant to paragraph (2), it will notify its customers of a breach of those customers' CPNI.

(4) Recordkeeping. The Company will maintain a record, electronically or in some other manner, of any breaches discovered, notifications made to the USSS and the FBI pursuant to paragraph (2), and notifications made to customers. The record will 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. The Company will maintain the record for a minimum of 2 years.

(5) Strict controls are in place involving responses to law enforcement agencies that serve the Company with valid legal demands, such as a court ordered subpoena, for CPNI. The Company will not supply CPNI to any law enforcement agency that does not produce a valid legal demand.