February 24, 2014

TRANSMITTED VIA ECFS

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

Re: Annual CPNI Certification
EB Docket No. 06-36
Xfone USA, Inc.

Dear Ms. Dortch:

In compliance with the FCC's Public Notice, DA 14-138 (released on February 5, 2014), Xfone USA, Inc., hereby files its annual CPNI officer certification and accompanying statement.

Should you have any questions or need additional information, please contact me via telephone at 806-788-2915 or via e-mail at danw@ntscom.com.

Respectfully submitted,

Daniel Wheeler

Enc

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

**EB Docket 06-36**

Annual 64.2009(e) CPNI Certification for 2013

Date filed: February 24, 2014

Name of company covered by this certification: Xfone USA, Inc.

Form 499 Filer ID: 825483

Name of signatory: Niv Krikov

Title of signatory: Treasurer and Chief Financial Officer

I, Niv Krikov, 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 adopted 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 the actions that the company has taken to establish operating procedures that ensure that the company is in compliance with the requirements set forth in section 64.2001 *et seq.* of the Commission's rules.

The company has not taken any actions (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 does not possess any information with respect to the processes pretexters are using to attempt to access CPNI.

The company has not received any customer complaints in the past year concerning the unauthorized release of CPNI.

Signed: _____

Niv Krikov
Treasurer and CFO

**Attachment A**

STATEMENT OF CPNI OPERATING PROCEDURES

Every employee of Xfone USA, Inc. (the "Company") has a duty to protect the confidentiality of customer proprietary information ("CPNI"), as defined in 47 U.S.C. § 222(f). A violation of the Company's operating procedures will result in disciplinary action which may result in immediate dismissal without warning.

The Company provides both local exchange service and long distance telephone service. It is the Company's policy to not use CPNI for any prohibited sales or marketing activity.

No Company employee shall disclose CPNI to any Company affiliate or other third party unless such disclosure is required by a lawful subpoena or is used for the following purposes: (1) to bill or collect payment for the Company's services or (2) to protect the rights or property of the Company or its customers. A Company employee that receives or obtains CPNI for the purpose of providing any telecommunications service shall use such information only for such purpose, and shall not use such information for any prohibited marketing purpose. A Company employee shall disclose CPNI only as permitted under Xfone's CPNI Policy attached to this document as **Exhibit 1.**[1]

The Company keeps a record of all instances where CPNI is disclosed or provided to third parties, or where third parties are allowed access to CPNI (hereinafter referred to as "the CPNI record"). An employee that discloses CPNI to a third party or allows a third party access to CPNI must add to the CPNI record the name and address of the third party, a description of the reasons for the disclosure of the CPNI, the specific

[1] The Company has adopted the CPNI Policy of its affiliate, NTS Communications, Inc., titled the NTS CPNI Policy

CPNI that was disclosed, and any written authorization from the customer to disclose the CPNI. The Company maintains this record for a minimum period of one year. In the event of a security breach that results in the unauthorized disclosure of CPNI, the Company will take all steps outlined in 47 C.F.R. § 64.2011. In addition, the Company will retain a record of any breach and the Company's response for a minimum of two (2) years.

All Company employees are required to sign a Confidentiality Agreement that obligates them to protect customer information. Employees are also required to sign a separate statement that they will comply with CPNI rules contained in NTS' Business and Marketing Code of Conduct. Employees who regularly deal with customers receive specific training on the CPNI Policy set out in **Exhibit 1** and are required to sign a statement that they understand it and that they will comply. Employees who regularly handle customer inquiries are also subject to live monitoring to ensure compliance and as necessary receive periodic reminders via e-mail or direct instruction from a supervisor.

Should the Company make a decision to modify its prohibition on the use of CPNI for marketing purposes, it will notify all employees of any such modifications. Under no circumstances will CPNI be used for any marketing purpose until after the Company has sent customers the notices required by 47 C.F.R. § 64.2008 and received the customer opt-in or opt-out approvals required for such use of CPNI. If the Company changes its current policy and decides to use CPNI in an out-bound sales or marketing campaign, the Company will establish a system which meets the requirements of 47 C.F.R. § 64.2009 (c) and (d).

Attachment A – Exhibit 1

## NTS CPNI Policy

Effective December 1, 2007, all telephone companies will be required to employ extra security measures to protect the privacy of customer call detail records and prevent disclosure to unauthorized persons.

Protection from Pretexting

These security measures have been mandated by the FCC in response to complaints of "pretexting" and other various invasions of the privacy of communication records. Pretexting is the practice of pretending to be a customer in order to obtain access to that customer call detail or other private communication records.

The Information that's Protected

The information these security measures are designed to protect is more commonly known as Customer Proprietary Network Information or CPNI for short. CPNI is defined as "any personally identifiable information derived from a customer's relationship with a provider of communications services." In other words, it is any information we possess about our customers.

Summary of Security Measures

In order to avoid confusion, NTS will replace its current authentication procedures with the security measures mandated by the FCC. What follows is a list of the steps that must be taken to authenticate that you are speaking to the customer, or, for business customers, their authorized representative. Compliance with any one of these steps will permit you to perform all account services for the customer.

Requests by Customers

Call Back. Call the customer at the Telephone Number of Record (the primary telephone number listed on the account). You must then authenticate the customer by any of the following: last four digits of their social security number, address on the account, or amount of last month's bill.

Password. You must request the customer's Password. If the customer is unable to provide you with their Password, you may assist them in obtaining a Password. These procedures are described below under the heading, Establishing Passwords.

Online Access. If the customer is unable to provide a Password or PIN, you may ask if they have established online access to their account. If they have, you may direct them to access the information on the Internet. If customers have not established online access to their account and wish to do so, you may instruct them to establish online access they will need a Personal Identification Number

(PIN) to establish online access. So, you may assist them in obtaining a PIN by following the procedures described below under the heading, Personal Identification Numbers.

Direct Mail. You may send the requested information to the customer's address of record (physical or e-mail listed on the account) via US or electronic mail.

In Person. The customer may appear in person and present a valid photo ID.

Requests by Non-Customers and Law Enforcement

All requests by non-customers (attorneys, relatives, guardians, powers of attorney, etc.) or Law Enforcement should be directed to the General Counsel whose contact information is available on the Intranet.

Personal Identification Numbers (PINs)

A PIN is a random number assigned to customers and located in the customer's account. A PIN is used to establish a Password. If a customer is unable to provide you with a PIN, you may provide it to them by any of the following methods:

Call Back: Call the Customer at the Telephone Number of Record (the primary telephone number listed on the account). The PIN may be communicated directly to the customer (after confirming the last four digits of the customer's social security number, address on the account, or the amount of the last month's bill), or the PIN may be left on an answering machine. As a practical matter, if you Call Back and after authentication speak to the customer, you may proceed to establish a Password or you may communicate the PIN for purposes of establishing online access.

Direct Mail. Send it to the customer's address of record (physical or e-mail address listed on the account) via US or electronic mail.

In Person. If the customer appears in person and presents a valid photo ID, you may give them their PIN.

Establishing Passwords

To establish a Password, customers must be available for Call Back, present their PIN, or appear in person and present a valid photo ID.

Call Back. You may establish a Password by calling the customer at the Telephone Number of Record (the primary telephone number listed on the account). If the customer answers, you may establish the Password after confirming any of the following: last four digits of their social security number, address on the account, or amount of last month's bill.

Once the customer provides the PIN or appears in person and presents a valid photo ID, they may set up a Password.

If the customer does not have a PIN, you may provide it to them by following the procedures under Personal Identification Numbers, above.

When customers establish a Password, you should also complete the "shared secret questions." These should be used if the customer has established a Password but is unable to remember it.

Report of Unauthorized Disclosures

If you are aware of any unauthorized disclosure of CPNI, you must report it immediately via e-mail to your immediate supervisor with a copy to generalcounsel@ntscom.com.

Enforcement

Compliance with these security measures and reporting requirements will be strictly enforced. Any failure to follow these requirements will result in disciplinary action in accordance with NTS Employee Policy Manual.

Exceptions

As is the case with any policy, circumstances will arise which are not addressed by this Policy. If you are presented with a situation that is not addressed by this Policy, you should notify your immediate supervisor.