



February 26, 2018

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 47 C.F.R. Section 64.2009(e), **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](mailto:danw@ntscom.com).

Respectfully submitted,

A handwritten signature in blue ink, appearing to read "Daniel Wheeler", followed by a checkmark.

Daniel Wheeler

Enc

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

**EB Docket 06-36**

Annual 64.2009(e) CPNI Certification for 2017

Date filed: February 26, 2018

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

Form 499 Filer ID: 825483

Name of signatory: Donald R. Pittman


Title of signatory: Treasurer and Chief Financial Officer

I, Donald R. Pittman, 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: 

Donald R. Pittman  
Treasurer and Chief Financial Officer

## **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(h). 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 provide or market service offerings, or alternate versions of existing service, which may include additional or related offerings, within the category of service (i.e., local, interexchange) to which the customer already subscribes; (2) to provide optional extended area calling plans; (3) 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 ID, call forwarding, and certain Centrex features; (4) to provide inside wiring installation, maintenance, or repair services; (5) to initiate, render, bill for, or collect for customer-authorized telecommunications services; (6) to protect the rights or property of NTS; (7) to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services; or (8) to market services other than those to which a customer already subscribes, or alternate versions of existing service, which may include additional or related offerings, if such customer contacts NTS to inquire about such service offerings. A Company employee that receives or obtains

CPNI for the purpose of providing any telecommunications service shall use such information only for such purposes. A Company employee shall disclose CPNI only as permitted under NTS' CPNI Policy attached to this document as **Exhibit 1**.<sup>1</sup>

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 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 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.

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. The Company will keep a record of all marketing campaigns which use its Customer's CPNI.

---

<sup>1</sup> The Company has adopted the CPNI Policy of its affiliate, NTS Communications, Inc., titled the "NTS CPNI policy."

The record will include a description of each campaign, the CPNI that was used, and the products and services that were offered. The Company will maintain the record for a period of one (1) year.

## **Attachment A – Exhibit 1**

### **NTS CPNI Policy**

#### **I Safeguards on Disclosure of CPNI**

Effective December 1, 2007, all telephone companies were required to employ extra security measures to protect the privacy of customer call detail records and prevent disclosure to unauthorized persons. In May 2015, this requirement was extended to broadband service providers.

#### **Protection from Pretexting**

Originally, these security measures were 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 adopted the security measures mandated by the FCC for access to all customer information. 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.

**Security Code.** You must request the customer’s Security Code. If the customer is unable to provide you with their Security Code, you may assist them in obtaining a Security Code. These procedures are described below under the heading, Establishing Security Codes.

**Online Access.** If the customer is unable to provide a Security Code 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 Jessica Salazar or Daniel Wheeler. Their 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 Security Code. 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 Security Code 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 Security Codes

To establish a Security Code, 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 Security Code 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 Security Code 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 Security Code.

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 Security Code, you should also complete the "shared secret questions." These should be used if the customer has established a Security Code 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@ntsc.com](mailto:generalcounsel@ntsc.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.

## II Approval Required for the Use of CPNI

#### Opt-out Approval

Notice. The Company will notify customers via mail prior to the use, disclosure or access to the customer's CPNI by the Company, its agents or affiliates in order to market communications-related services to the customer.

Opt-out Approval means that a customer is deemed to have consented to the use, disclosure, or access to the customer's CPNI if the customer fails to object within the period of time stated on the Customer's notice.

Customers may call in at any time to Opt-out of the following uses of the customer's CPNI:

- (1) to provide or market service offerings, or alternate versions of existing service, which may include additional or related offerings, within the category of service (i.e., local, interexchange) to which the customer already subscribes;
- (2) to provide optional extended area calling plans; or
- (3) 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 ID, call forwarding, and certain Centrex features;



Customers may not Opt-out of the following uses of the customer's CPNI:

- (1) to provide inside wiring installation, maintenance, or repair services;
- (2) to initiate, render, bill for, or collect for customer-authorized telecommunications services;
- (3) to protect the rights or property of the Company;
- (4) to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services; or
- (5) to market services other than those to which a customer already subscribes, or alternate versions of existing service, which may include additional or related offerings, if such customer contacts the Company to inquire about such service offerings

Recording Opt-out Approval. Customers who call in to Opt-out, mark the appropriate field in the customer's account.

#### Opt-in Approval

Notice. The Company will notify customers via mail prior to the use, disclosure or access to the customer's CPNI by any third party who is not affiliated with the Company for any purpose.

Opt-in Approval requires the customer to provide affirmative, express consent allowing the use, disclosure or access to the customer's CPNI.

Customers will be required to provide Opt-in Approval for any use, disclosure or access to the customer's CPNI by third parties who are not affiliated with the Company.

Recording Opt-in Approval. Customers who call to Opt-in, mark appropriate field in the customer's account.