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

EB Docket 06-36

Annual 64.2009(e) CPNI Certification for 2014

Name of company covered by this certification: **Ptera Inc.**

Form 499 Filer ID: **830799**

Name of signatory: **James Wilson**

Title of signatory: **Chief Executive Officer**

I, James Wilson, certify that I am an officer of Ptera Inc. (collectively, "the Company"), 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 is an accompanying statement from the Company's employee manual identifying policies of the Company that have been enacted to comply with the CPNI 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 Federal Communications Commission) against data brokers during 2014. The Company is not aware of any attempt by pretexters to access CPNI held by the Company during 2014.

The Company has not received any customer complaints in 2014 concerning the unauthorized release of CPNI. Nor is the Company aware of any instances involving unauthorized disclosure of CPNI or improper access of CPNI by Company employees or access by individuals not authorized to receive or view the information.

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.

Printed Name: James Wilson

Position: Chief Executive Officer

Signature: James Wilson

Date: April 14, 2015

CPNI - Protecting our customer's data

Ptera policy requires that our customer data be protected at each stage of the customer acquisition and maintenance process.

This is accomplished through:

1- Proper entry of the customer's information into our CMS

2- Protection of access to customer information through good password management practices

3- Proper identification of the customer at each interaction

4- Locked filing cabinets of any written customer information and contracts in a locked room

5- We don't retain any unneeded customer information such as SSN. Customer credit card information is not entered except through the payment portal and is not written down.

6- Ptera servers are located in multiple sites with physical access control and password protection. Company firewalls control outside access to these devices.