Annual 47 CFR § 64.2009(e) CPNI Certification

EB Docket 06-36

Annual 64.2009(e) CPNI Certification for 2018 covering the prior calendar year 2017.

1. Date filed: February 16th, 2018
2. Name of company(ies) covered by this certification: Orlando Telephone Company, Inc. dba Summit Broadband
3. Form 499 Filer ID: 819915
4. Name of signatory: Paula Meads
5. Title of Signatory: VP Finance
6. Certification:

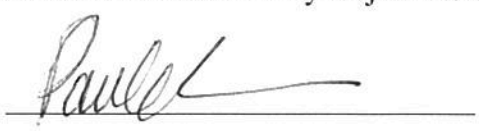
I, Paula Meads, certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. *See* CFR § 64.2001 *et seq.*

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, safeguards, recordkeeping, and supervisory review) set forth in section 64.2001 *et. seq.* of the Commission's rules.

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 CFR § 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 

Attachments: Accompanying Statements explaining CPNI procedures

ORLANDO TELEPHONE COMPANY, INC DBA SUMMIT BROADBAND
ACCOMPANYING STATEMENT TO CPNI CERTIFICATION
February 16th, 2018

This statement explains how Orlando Telephone Company, Inc. dba Summit Broadband (the "Company's") procedures ensure compliance with the FCC CPNI rules as set forth in 47 CFR § 64.2001 *et seq*.

1. The Company has a written CPNI policy that explains what CPNI is, when it may be used without customer approval, and when customer approval is required prior to CPNI being used, disclosed, or accessed for marketing purposes.

2. The Company has established as system by which the status of a customer's approval for use of CPNI, as defined in 47 USC 222(h)(1), can be clearly established prior to the use of CPNI. The Company relies on the involvement of its high-level management to ensure that no use of CPNI is made until a full review of applicable law has occurred.

3. The Company has trained its personnel regarding when they are authorized to use CPNI, as well as when they are not authorized to use CPNI. Employees with access to this information are familiar with the FCC's rules and are prohibited from disclosing or permitting access to CPNI without the appropriate customer consent. The Company has an express disciplinary process in place for personnel who make unauthorized use of CPNI. In accordance with Company policy, any employee who uses, discloses, or permits access o CPNI in violation of Federal regulations is subject to disciplinary action, including possible termination.

4. The Company has assigned a CPNI Compliance Officer and CPNI Compliance Administrator to serve as the central points of contact regarding the Company's CPNI responsibilities and questions related to CPNI policy. The CPNI Compliance Officer has responsibilities including, but not limited to, supervising the training of all Company employees with access to CPNI, investigating complaints of unauthorized release of CPNI, and reporting any breaches to the appropriate law enforcement agencies and customers in compliance with the FCC's CPNI rules. The CPNI Compliance Officer also maintains records in accordance with FCC CPNI rules, including records of any discovered breaches, notifications of breaches to law enforcement, and law enforcements' responses to the notification, for a period of at least two (2) years.

5. Appropriate safeguards on the disclosure of CPNI have been implemented in accordance with CFR § 64.2010. Prior to the disclosure of CPNI, customers initiating calls to or visiting the Company's offices are properly authenticated. Passwords and password back-up authentication procedures for lost or forgotten passwords are implemented in accordance with CFR § 64.2010(e). To establish a password for an existing customer, the Company must first authenticate the customer without the use of readily available biographical information, or account information, such as calling the customer back at their telephone number of record. For a new customer the password is established at the time of service initiation.

6. Call detail information is only disclosed over the telephone, based on customer-initiated telephone contact, if the customer first provides a password that is not prompted by the

Company asking for readily available biographical information, or account information. If the customer does not provide a password, or responses to back-up authentication questions when the password has been forgotten or lost, call detail is only provided by sending it to the customer's address of record or by calling the customer at their telephone number of record. If the customer is able to provide call detail information to the Company without the Company's assistance during a customer-initiated call, then the Company is permitted to discuss only that call detail information provided by the customer.

7. Prior to the Company disclosing CPNI to a customer visiting any of its retail offices in person, the customer must present a valid photo ID matching the customer's account information.

8. The Company does not rely on readily available biographical information or account information to authenticate a customer's identity before a customer can access CPNI related to their telecommunications account online. Once authenticated, a customer can obtain online access to CPNI related to his or her telecommunications account with a password that is not prompted by the Company asking for readily available biographical information or account information.

9. The Company has implemented procedures to notify customers immediately whenever a password, customer response to a back-up means of authentication for lost or forgotten passwords, or address of record is created or changed.

10. The Company's policy is to maintain records of its own sales and marketing campaigns that use CPNI. The Company likewise maintains records of its affiliates' sales and marketing campaigns that use CPNI. The Company also maintains records of all instances where CPNI was disclosures or provided to third parties, or where third parties were allowed access to CPNI. These records include a description of each campaign, the specific CPNI that was used in the campaign, and the products and services that were offered as part of the campaign. The Company maintains these records in its offices for a minimum of one (1) year.

11. The Company's policy is to maintain records of customer approval for use of CPNI, as well as notices required by the FCC's regulations, for a minimum of one (1) year. The company maintains records of customer approval and disapproval for use of CPNI in a readily-available location so the status of customer's approval can be clearly established prior to the use of CPNI.

12. The Company's policy is to maintain records of a CPNI breach for a minimum of two (2) years. These records will include a description of the steps the Company took to prevent the breach, how the breach occurred, the impact of the breach, and proof of notification to law enforcement and the customer, if applicable.

13. The Company has a supervisory review process regarding compliance with the FCC's rules relating to protection of CPNI for outbound marketing situations. The purpose of this supervisory review process is to ensure compliance with all rules prior to using CPNI for a purpose for which customer approval is required. The Company's sales personnel must obtain supervisory approval of any proposed outbound marketing request for customer approval.

14. The Company's CPNI Compliance Officer oversees the use of opt-in, opt-out, or any other approval requirements, or notice requirements (such as notification to the customer of the right to restrict use of, disclosure of, and access to CPNI), contained in the FCC's regulations. The CPNI Compliance Officer also reviews all notices required by the FCC regulations for compliance therewith.

15. The Company will provide written notice within five (5) business days to the Commission of any instance where the opt-out mechanisms do not work properly, to such a degree that customers' inability to opt-out is more than an anomaly. The notice will be in the form and content required by CFR § 64.2009(f)(1) and will be submitted even if the Company offers other methods by which customers may opt-out.

16. The Company enters into confidentiality agreements, as necessary, with any joint venture partners or independent contractors to whom it discloses or provides access to CPNI. The Company requires express opt-in consent from a customer prior to the release of CPNI to a joint venture partner or independent contractor for marketing purposes.