Annual 47 C.F.R. § 64.2009(e) CPNI Certification
EB Docket 06-36

Annual 64.2009(e) CPNI Certification for 2018

Date filed: March 1, 2019

Name of company covered by this certification: SpeedConnect LLC

Form 499 Filer ID: 830691

Name of signatory: John Ogren

Title of signatory: CEO / President

I, John Ogren, certify that I am an officer SpeedConnect LLC ("SpeedConnect" or the "Company"), and acting as an agent of SpeedConnect, that I have personal knowledge that SpeedConnect 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 SpeedConnect's procedures ensure that the Company is in compliance with the requirements (including, where applicable, those mandating the adoption of CPNI procedures, record keeping and supervisory review) set forth in section 64.2001 *et seq.* of the Commission's rules.

SpeedConnect has not taken any actions (i.e., proceedings instituted or petitions filed by SpeedConnect at either state commissions, the court system, or at the Commission) against data brokers in the past year, nor is there any evidence that pretexters attempted to access CPNI maintained by SpeedConnect.

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

Signed

John Ogren
CEO and President
SpeedConnect LLC

SPEEDCONNECT LLC STATEMENT
OF COMPLIANCE WITH CPNI RULES

SpeedConnect LLC ("SpeedConnect" or the "Company") provides interconnected Voice over Internet Protocol ("VoIP") service over dedicated facilities to enterprises, including businesses, schools and hospitals, and carrier customers. SpeedConnect's VoIP contracts contain confidentiality agreements that address use and protection of customers' private information.

Consistent with the CPNI rules, the Company may use, disclose and permit access to CPNI without customer approval (1) to render, bill and collect for services provided; (2) to protect rights or property of the Company, other users or other carriers from unlawful use; (3) for the purpose of network maintenance, repair and troubleshooting; and (4) to comply with a valid legal process such as a subpoena, court order, or search warrant.

The Company does not use, disclose or permit access to CPNI for marketing purposes other than for the purpose of providing service offerings for the type of services to which the Company's customer already subscribes. It is therefore not required to seek approval from existing customers to use their CPNI and does not maintain a record of a customer's approval to use CPNI. In the event that the Company changes its marketing practices such that opt-out notices are required, the Company will implement procedures to ensure that customers are notified about the new practices and the customer's approval can be established prior to use of CPNI. Furthermore, the Company does not share, sell, lease or otherwise provide CPNI to any of its affiliates, suppliers, vendors and any other third parties for the purposes of marketing any services.

The Company has implemented processes and procedures to train its personnel as to when they are and are not permitted to use CPNI and has completed such training and will periodically refresh such training (at minimum, annually). For instance, all employees with access to the information receive CPNI training and are required to abide by the Company's CPNI Policy, which, *inter alia,* requires employees to maintain the confidentiality of CPNI. The Company's CPNI Policy also provides a roadmap of how Company employees are required to use, maintain and disclose CPNI. Those individuals who have access to customer's CPNI have specific performance requirements related to use and protection of CPNI and are subject to supervisory review. Employees who violate the Company's CPNI Policy are subject to disciplinary action, which will vary depending upon the severity of the violation(s).

The Company has established a supervisory review and approval process to ensure that any future marketing campaigns are consistent with FCC's CPNI rules. The Company maintains a record for at least one year of its own and, if applicable, affiliates' sales and marketing campaigns, if any, that use customers' CPNI.

SpeedConnect has elected not to disclose CPNI over the phone and does not allow for online access to CPNI. SpeedConnect operational procedures require that all

requests for customer CPNI be in writing, whether from an authorized employee, third party or law enforcement, and these requests are maintained in SpeedConnect archives for at least one year. The Company practice is to maintain a record of all instances where CPNI was disclosed or provided to third parties, or where third parties were allowed access to CPNI. Requests for CPNI by law enforcement agencies are only granted if a subpoena or court order is submitted by an authorized court or government agency, or if the customer provides written permission, which shall be directed to an officer of the Company, or its designee, for approval before such access is granted by Company employees or agents.

In the case of a breach which results in unauthorized CPNI disclosure, SpeedConnect sends notification of such breach to the governmental agencies and to the customer as specified in the FCC CPNI Rules; that is, no later than seven days following the breach, to the United States Secret Service (USSS) and the Federal Bureau of Investigation (FBI) in accordance with 47 C.F.R. § 64.2011. SpeedConnect's internal procedure is to notify the customer following notice to law enforcement, unless there is an urgent need to notify the customer to prevent harm or law enforcement directs SpeedConnect to withhold any public disclosure for up to 30 days. SpeedConnect retains electronic or manual records of all CPNI breaches for a minimum of two years.