ANNUAL 47 C.F.R. § 64.2009(e) CPNI CERTIFICATION

EB DOCKET 06-36

Annual 64.2009(e) CPNI Certification for 2010 covering the prior year 2009

Date Filed: February 4, 2010

Name of company covered by this certification: Cordia Communications Corp.

Form 499 Filer ID: 821630

Name of executing officer: Wesly Minella

Title of signatory: Secretary

CERTIFICATION

I, Wesly Minella, hereby 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* 47 C.F.R §§ 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 set forth in § 64.2001 *et seq.* of the Commission's rules.

The company has not taken any actions (proceedings instituted or petitions filed by a company 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 required 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.

Wesly Minella, Secretary

Attachment: Accompanying Statement explaining CPNI procedures

CORDIA COMMUNICATIONS CORP'S
STATEMENT OF CPNI PROCEDURES

The Company recognizes its duty to protect customer proprietary network information ("CPNI") and believes that is operating procedures, set forth below, ensure compliance with the requirements set forth in section 64.2001 *et seq.* regarding the protection of.

- Company will not disclose CPNI to unauthorized persons, nor may it utilize CPNI in certain ways without the consent of our customers. Prior to providing customers with their own CPNI we must authenticate the customer.
    - Telephone – call detail information may not be released until Company has obtained the account password from the caller or calls the customer back at the BTN of record to ensure the customer is who they claim to be. Non call detail information may be released after the Company calls the customer back to authenticate identity.
    - In person - CPNI may be released to customers, in person that provide a valid government issued photo ID. The name on the photo ID must match the name on the account
- Company recognizes several exceptions that permit disclosure of CPNI with consent:
    - Internal administrative use to allow the Company to initiate, render invoices and collect amounts due for services provided to customers;
    - To protect the interests of the Company, namely to prevent fraud or illegal use of our systems and network;
    - If required by law through valid subpoena or other legal process and in response to valid legal requests from law enforcement.
- Company continually educates and trains its employees regarding the appropriate use of CPNI. In the event that an employee's actions fail to conform to these standards the appropriate disciplinary measures shall be taken
- Company does not utilize CPNI to identify or track customers that call competing service providers
- In the event that an unauthorized disclosure of CPNI occurs, Company will promptly notify law enforcement and the customer of the unauthorized disclosure
- Company understands that it is required to notify customers when changes have been made to passwords, customer responses to back-up means of authentication, or addresses of record by mailing a notification to the account address of record; the Company does not reveal the changed data in the notification.