February 28, 2011

Marlene H. Dortch
Office of the Secretary
Federal Communications Commission
445 12th Street, SW, Suite TW-A325
Washington, DC 20554

RE: RCN Telecom Services (Lehigh) LLC (ID 828462)

RCN BecoCom, LLC (ID 814887)

RCN Telecom Services of Illinois, LLC (ID 820149)

RCN Telecom Services of Philadelphia, LLC (ID 812061)

RCN Telecom Services of New York, LP (ID 828461)

Starpower Communications, LLC d/b/a RCN (ID 817208)

RCN New York Communications, LLC* (ID 822434) – *Certified through Aug. 25, 2010*

NEON Optica, Inc.* (ID 821446) – *Certified through August 25, 2010*

Annual CPNI Compliance Certification, EB Docket No. 06-36

Dear Secretary Dortch:

Attached for filing in EB Docket No. 06-36, please find the Annual 47 C.F.R. § 64.2009(e) CPNI Compliance Certificate and accompanying statement of RCN Telecom Services (Lehigh) LLC, RCN BecoCom, LLC, RCN Telecom Services of Illinois, LLC, RCN Telecom Services of Philadelphia, LLC, RCN Telecom Services of New York, LP, and Starpower Communications, LLC d/b/a RCN (collectively, "RCN").

*Further, this Compliance Certificate shall include the business activities of RCN New York Communications, LLC, and NEON Optica, Inc. (collectively, "Sidera"), but only through August 25, 2010.

For clarification, on March 5, 2010, RCN Corporation and ABRY Partners, LLC, announced a merger agreement which provided for an investment fund managed by ABRY to acquire RCN Corporation and its various operating subsidiaries. Upon closing of the transaction, which was effectuated on August 26, 2010, RCN Corporation was separated into two (2) distinct operating units, each operating under separate management. These operating units are known as RCN Telecom Services, LLC, and Sidera Networks.

Effective August 26, 2010, RCN Telecom Services, LLC, is the parent company to the aforementioned "RCN" entities in paragraph 1 above, while Sidera Networks is the parent company to those entities in paragraph 2 above. To reaffirm, as a result of the merger RCN and Sidera Networks are operating under separate management.

As such, please take note that this filing incorporates the aforementioned ***pre-merger*** business units of RCN New York Communications, LLC (Filer ID 822434), and NEON Optica, Inc. (Filer ID 821446) for the calendar year 2010, however only up to and including the date of August 25, 2010. RCN does not make any certification as to Sidera Networks compliance after August 25, 2010.

If there are questions regarding this filing, please contact the undersigned. Thank you for your assistance.

Sincerely,
RCN

Robert Roeder
SVP Network Services

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

EB Docket No. 06-36

Annual 64.2009(e) CPNI Certification for 2010

Date filed: February 28, 2011

Certifying Companies with Form 499 Filer IDs:

RCN Telecom Services (Lehigh) LLC (ID 828462)

RCN BecoCom, LLC (ID 814887)

RCN Telecom Services of Illinois, LLC (ID 820149)

RCN Telecom Services of Philadelphia, LLC (ID 812061)

RCN Telecom Services of New York, LP (ID 828461)

Starpower Communications, LLC d/b/a RCN (ID 817208)

RCN New York Communications, LLC* (ID 822434) – *Certified through Aug 25, 2010*

NEON Optica, Inc.* (ID 821446) – *Certified through August 25, 2010*

Name of signatory: Robert Roeder

Title of signatory: SVP, Network Services

I, Robert Roeder, certify that I am an officer of RCN Telecom Services (Lehigh) LLC, RCN BecoCom, LLC, RCN Telecom Services of Illinois, LLC, RCN Telecom Services of Philadelphia, LLC, RCN Telecom Services of New York, LP, and Starpower Communications, LLC d/b/a RCN (collectively, "RCN" or "the company"), and acting as an agent of the company, I have personal knowledge that RCN 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.*

*Furthermore, pursuant to the explanation below, I certify that up to and including the date of August 25, 2010, I had personal knowledge of the operating procedures that are adequate to ensure compliance with the aforementioned CPNI rules as to RCN New York Communications, LLC, and NEON Optica, Inc. (collectively also "the company", only through August 25, 2010).

On March 5, 2010, RCN Corporation and ABRY Partners, LLC, announced a merger agreement which provided for an investment fund managed by ABRY to acquire RCN Corporation and its various operating subsidiaries. Upon closing of the transaction, which was effectuated on August 26, 2010, RCN Corporation was separated into two (2) distinct operating

units, each operating under separate management. These operating units are known as RCN Telecom Services, LLC, and Sidera Networks.

Effective August 26, 2010, RCN Telecom Services, LLC, is the parent company to the aforementioned "RCN" entities in paragraph 1 above, while Sidera Networks is the parent company to those entities in paragraph 2 above. To reaffirm, as a result of the merger RCN and Sidera Networks are operating under separate management.

Therefore, please take note that this filing incorporates the aforementioned ***pre-merger*** business units of RCN New York Communications, LLC (Filer ID 822434), and NEON Optica, Inc. (Filer ID 821446) for the calendar year 2010, however only up to and including the date of August 25, 2010. RCN does not make any certification as to Sidera Networks compliance after August 25, 2010.

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 section 64.2001 *et seq.* of the Commission's rules.

RCN 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 in the past year. RCN has no information to report with respect to the processes pretexters are using to attempt to access CPNI. Furthermore, RCN's steps taken to protect CPNI are described in the accompanying statement.

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

By: _____

Robert Roeder
SVP Network Services

RCN
February 28, 2011

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

EB Docket No. 06-36

RCN submits this accompanying statement to explain how the company's procedures ensure that the company is in compliance with the substantive requirements set forth in section 64.2001 *et seq.* of the Commission's rules.

1. Compliance with § 64.2007, approval required for use of customer proprietary network information:

In those instances in which customer approval is required for use of CPNI, RCN obtains approval through oral and/or written methods. RCN obtains opt-out approval as described in item 2, below. RCN does not currently use CPNI for any purpose for which opt-in approval is required under the Commission's rules, with the exception of per-call opt-in approval as described in item 2 below. The customer's approval or disapproval to use, disclose, or permit access to a customer's CPNI obtained by RCN remains in effect until the customer revokes or limits such approval or disapproval. Records of customers' CPNI approvals are kept per RCN's standard operating procedures, which amount to a period of at least one year.

2. Compliance with § 64.2008, notice required for use of customer proprietary network information:

Prior to soliciting the customer's continuing opt-out approval for use of CPNI, RCN provides written notification of the customer's right to restrict use of, disclosure of, and access to that customer's CPNI. The content of such notification complies with the Commission's rules. RCN keeps records of notification for at least one year. Opt-out notices are provided to customers every year, and customers are given a minimum of 30-days to opt-out before they are presumed to have consented to use of their CPNI. For one-time use of CPNI on inbound and outbound customer telephone contacts for the duration of the call only (per-call opt-in), RCN's representatives obtain oral consent from the customer pursuant to a customer service script that complies with the Commission's rules.

3. Compliance with § 64.2009, safeguards required for use of customer proprietary network information:

RCN has a system in place by which the status of a customer's CPNI approval can be clearly established prior to the use of CPNI. Specifically, RCN identifies all customers who have opted-out of use of their CPNI by so noting on their account record in the database supporting RCN's convergent voice, video, and data billing and customer care solution management system.

RCN then compares all marketing lists against those customers identified as having opted-out through the company's account records database. Personnel are trained as to when they are and are not authorized to use CPNI, and RCN has a disciplinary process in place for noncompliance. A record in compliance with the Commission's rules is kept for a minimum of one year of RCN and its affiliates' marketing campaigns that use our customers' CPNI and instances in which our customers' CPNI is disclosed or provided to, or accessed by, third parties.

In addition, RCN has in place and keeps records for a minimum of one year of a review process regarding compliance with the rules for outbound marketing situations, which requires sales personnel to obtain approval of any proposed outbound marketing request for customer approval.

4. Compliance with § 64.2010, safeguards on the disclosure of customer proprietary network information:

RCN has physical security, information technology, and personnel measures in place to discover and protect against attempts to gain unauthorized access to CPNI. With the exception of business customers that have both a dedicated account representative and a contract that specifically addresses protection of CPNI, customers are asked to establish a password and provide answers to back-up security questions that do not use readily available biographical information, or account information.

Customers who forget their password and cannot provide the answer to their back-up security questions to retrieve their password are required to be re-authenticated to establish a new password and new answers to back-up security questions. Passwords are required for a customer to obtain online access to CPNI, and prior to disclosure to the customer of call detail information over the telephone. Customers who do not have a password may have RCN send call detail and other account information to the customer's address of record. Customers requesting CPNI at one of RCN's retail locations must present a valid photo ID matching the customer's account information.

In the event a password, customer answer to a back-up security question, online account, or address of record is created or changed, RCN immediately provides notice to the customer at the pre-existing address of record via US Mail. Such notice informs the customer as to the nature of the change, but does not reveal the changed information.

5. Compliance with § 64.2011, notification of customer proprietary network information security breaches:

RCN has not experienced any CPNI breaches during the reporting year. However, RCN has in place procedures to detect breaches and to notify law enforcement and customers, in compliance with the Commission's rules, should a breach occur. In the event of a breach, RCN has procedures in place to maintain a record of notifications to law enforcement and customers documenting the date(s) of discovery and notification, a detailed description of the CPNI that was the subject of the breach, and the circumstances of the breach.

When required in previous years, RCN has maintained a physical and electronic record of the notifications to law enforcement and the customers, as well as a more substantive summary of the circumstances and subject-matter of the breach. All records are and continue to be maintained for a minimum of two (2) years, in accordance with the Commission's rules.