RCN

DOCKET FILE COPY ORIGINAL

Received & Inspected
FEB 28 2014
FCC Mail Room

February 28, 2014

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)

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").

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

Sincerely,
RCN

Jeffrey B. Kramp
Senior Vice President, General Counsel & Corporate Secretary

No. of Copies rec'd 0+4
List ABCDE

RCN

Received & Inspected
FEB 28 2014
FCC Mail Room

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

EB Docket No. 06-36

Annual 64.2009(e) CPNI Certification for Calendar Year 2013

Date filed: February 28, 2014

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)

Name of signatory: Jeffrey B. Kramp

Title of signatory: Senior Vice President, General Counsel & Corporate Secretary

I, Jeffrey B. Kramp, 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 "Companies"), and acting as an agent of the Companies, 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*.

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 received one (1) customer complaint concerning the unauthorized release of CPNI in the past year, in RCN's New York market. To summarize, on or about August 5, 2013, a person purporting to be the customer/authorized user on the customer's account attempted several times to activate call forwarding on the account and have calls forwarded to a new telephone number. Ultimately, RCN activated call forwarding as requested, and in the process of

establishing this feature, a customer care representative provided this person with the CPNI passwords and answers to security questions for this account. The customer received mail from RCN that certain changes were made on the account, which prompted the customer to call RCN. Based on RCN's conversation with the customer, the new phone account was disconnected. This CPNI breach was reported to the Commission, all in accordance with the guidelines promulgated by the Commission and state/local governmental authorities.

By: _____

Jeffrey B. Kramp
Senior Vice President, General Counsel & Corporate Secretary

Received & Inspected
FEB 28 2014
FCC Mail Room

RCN
February 28, 2014

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 (1) 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 thirty (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 commercial 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 experienced one (1) CPNI breach during the reporting year. In this instance, and in all other instances, 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.