NextG Networks®

March 1, 2011

VIA ELECTRONIC FILING

Marlene H. Dortch
Office of the Secretary
Federal Communications Commission
445 12th Street, S.W.
Washington, DC 20554

Re: EB Docket 06-36 – 47 CFR § 64.2009(e) Annual CPNI Certification

Dear Ms. Dortch:

Pursuant to Section 64.2009(e) of the Commission's Rules, enclosed for filing in the above-referenced docket is the executed annual Customer Proprietary Network Information ("CNPI") Compliance Certificate of

NextG Networks Atlantic, Inc.,
NextG Networks of California, Inc.,
NextG Networks of Illinois, Inc., and
NextG Networks of NY, Inc.

Please also find attached to the certificate a summary of the companies' CPNI policies and procedures.

Respectfully submitted,

Robert A. Millar
Senior Regulatory Counsel
NextG Networks Atlantic, Inc.
NextG Networks of California, Inc.
NextG Networks of Illinois, Inc.
NextG Networks of NY, Inc.

cc: fcc@bcpiweb.com

enclosures

NextG Networks, Inc.
890 Tasman Drive, Milpitas, CA 95035-7439 • Tel 408.954.1580 • Fax 408.434.6285 • info@nextgnetworks.net • www.nextgnetworks.net

2011 Customer Proprietary Network Information Certification
Annual report covering calendar year 2010
EB Docket No. 06-36

1. Date Filed: February 28, 2011
2. Name of Companies covered by this certification and Form 499 Filer ID Numbers:

NextG Networks Atlantic, Inc.	824158
NextG Networks of California, Inc.	824160
NextG Networks of Illinois, Inc.	824164
NextG Networks of NY, Inc.	824162

3. Name of Signatory: Robert L. Delsman
4. Title of Signatory: Senior Vice President and General Counsel
5. Certification:

I, Robert L. Delsman, certify that I am an officer of the companies named above (collectively the "Company") and, acting as an agent of the Company, that I have personal knowledge that the Company has established operating procedures, summarized in the attached statement, that are adequate to ensure compliance with the Commission's customer proprietary network information ("CPNI") rules as set forth in 47 C.F.R. Section 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, recordkeeping, and supervisory review) set forth in Section 64.2001 *et seq.* of the Commission's rules.

The Company has not received any customer complaints in the past calendar year concerning unauthorized release of CPNI. The Company does not have any material information with respect to the processes pretexters are using to attempt to access CPNI that is not already a part of the record in the Commission's CC Docket No. 96-115. The Company has therefore not taken any actions in the past year against data brokers, including proceedings instituted or petitions filed by the Company at either state commissions, the court system, or at the Commission. The Company has established procedures to report any breaches to the FBI and the United States Secret Service, and it will continue to take reasonable measures to discover and protect against pretexting and other unauthorized access to CPNI.

I hereby represent and warrant that the above certification is consistent with Section 1.17 of the Commission's rules, 47 C.F.R. § 1.17, which requires truthful and accurate

statements to the Commission, and acknowledge that false statements and misrepresentations to the Commission are punishable under Title 18 of the United States Code and may subject the Company to enforcement action.

Robert L. Delsman
Senior Vice President and General Counsel
NextG Networks Atlantic, Inc.
NextG Networks of California, Inc.
NextG Networks of Illinois, Inc.
NextG Networks of NY, Inc.

Executed February 28, 2011

Revised CPNI Compliance Policies of NextG Networks

Effective December 8, 2007

NextG Networks Atlantic, Inc.; NextG Networks of California, Inc.; NextG Networks of Illinois, Inc.; and NextG Networks of NY, Inc. (collectively, "NextG") have implemented the following policies and procedures to protect the confidentiality of Customer Proprietary Network Information ("CPNI") and to assure compliance with the rules of the Federal Communications Commission ("FCC") set forth in 47 C.F.R. Part 64, Subpart U, Section 2001 *et seq*. NextG has revised its policies as of December 8, 2007 to implement the FCC's new rules adopted in *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information,* CC Docket No. 96-115, Report and Order and Further Notice of Proposed Rulemaking, FCC 07-22 (rel. April 2, 2007). NextG's policy is administered by its CPNI Compliance Officer, Robert L. Delsman.

CPNI is "(A) information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and (B) information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier."

NextG is a carrier's carrier that provides service only to other telecommunications carriers and not to end-user consumers. NextG executes specific nondisclosure agreement with all of its customers governing the confidentiality of the customer's information. Nonetheless, NextG's compliance with the FCC's CPNI rules is further demonstrated by the policies, practices, training, and audit procedures employed by NextG. Following is a brief explanation of the procedures NextG employs.

I. USE, DISCLOSURE OF, AND ACCESS TO CPNI

In accordance with Section 222(b) of the Act, 47 U.S.C. § 222(b), when NextG receives or obtains proprietary information from another carrier for purposes of providing a telecommunications service, it only uses such information for such purpose.

To the extent not inconsistent with Section 222(b), NextG may use, disclose, or permit access to CPNI in its provision of the communications service from which such information is derived; for services necessary to, or used in, the provision of such communications service, including to initiate, render, bill, and collect for telecommunications services; to protect the rights or property of NextG or to protect users or other carriers or service providers from fraudulent, abusive. or unlawful use of, or subscription to, such services; to provide installation, maintenance, or repair services; as required by law; or as expressly authorized by the customer.

NextG does not use CPNI for the purpose of marketing service offerings among different categories of service pursuant to 47 C.F.R. § 64.2005(a), because NextG only offers one category of service. NextG does, however, use CPNI to market service offerings among the same category of service to which the customer already subscribes.

Except as provided above, NextG will only release or disclose CPNI to a third party pursuant to a valid request from law enforcement, the federal judiciary, or other appropriate authority. For example, customer information will only be disclosed after the requesting party demonstrates that the request is made pursuant to a valid subpoena, court order, search warrant, or national security letter. In such event, NextG has a policy of providing its customers with ten (10) days' advance notice and an opportunity to object prior to releasing such information to third parties.

NextG does not use, disclose, or permit access to CPNI to identify or track customers that call competing service providers.

II. SAFEGUARDS AGAINST DISCLOSURE OF CPNI TO UNAUTHORIZED PARTIES

NextG has specific nondisclosure agreements with every customer that address the protection of the carrier's confidential information. NextG has a system that records each subscriber's individual privacy preferences and allows for changes to those preferences as validly requested by the subscriber. This system enables NextG to determine the status of a customer's CPNI requirements prior to the use of CPNI.

Because each such customer is a business customer and is able to contact their dedicated account representative directly without contacting a NextG call center, the business customer exemption set forth in 47 C.F.R. § 64.2010(g) applies and the FCC's requirements for authentication of inbound customer contacts do not apply. Even to the extent that the FCC's authentication requirements do apply, NextG does not provide CPNI to inbound callers, through online accounts over the Internet, or to visitors at a retail office. If NextG offers such access in the future, it will revise these policies as may be necessary to comply with the FCC's requirements for authentication of inbound callers, online users, and retail office visitors.

When an address of record is created or changed, NextG will send a notice to a preexisting customer address of record notifying them of the change. This notice requirement does not apply when the customer initiates service. The notice will not reveal the changed information and will direct the customer to notify NextG immediately if they did not authorize the change. There are no passwords, customer response to a back-up means of authentication for lost or forgotten passwords, or online accounts associated with CPNI possessed by NextG, so the other notice requirements set forth in 47 C.F.R. § 64.2010(f) are inapplicable.

Call detail information records are maintained in secure databases accessible only by a limited number of employees. To prevent unauthorized access to CPNI, NextG employees must use a unique login and password to obtain access to databases that include CPNI.

Above and beyond the specific FCC requirements, NextG will take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI. The FCC's rules require carriers on an ongoing basis to "take reasonable measures to discover and protect against activity that is indicative of pretexting." If any employee becomes aware of new methods that are being used or could be used by third parties to attempt to obtain unauthorized access to CPNI or of possible changes to NextG's existing policies that would strengthen protection of CPNI, he or she should report such information immediately to NextG's CPNI Compliance Officer so that NextG may evaluate whether existing policies should be supplemented or changed.

III. REPORTING CPNI BREACHES TO LAW ENFORCEMENT

Any NextG employee that becomes aware of any breaches, suspected breaches, or attempted breaches of CPNI must report such information immediately to the NextG CPNI Compliance Officer and must not report or disclose such information by any employee to any non-employee, including the potentially affected customer, except in express conformance with the procedures described below. Any employee that fails to report such information will be subject to disciplinary action that may include termination.

It is NextG's policy that employees should not be discouraged from reporting information about breaches that may have been caused in part by their own actions or omissions. Once a breach has occurred, the most important objective is to attempt to limit the damage to customers, make any adjustments as needed to prevent a recurrence of the breach, and to alert law enforcement promptly. Therefore, although employees who violate NextG's CPNI compliance policies are subject to discipline, the sanctions may be substantially reduced where employees promptly self-report violations if appropriate.

A. Identifying a "Breach"

A "breach" has occurred when any person, without authorization or exceeding authorization, has intentionally gained access to, used, or disclosed CPNI. If an employee has information about an incident and is not certain that the incident would not constitute a breach under this definition, the incident must be reported to the CPNI Compliance Officer.

If a NextG employee determines that an unauthorized person is attempting to gain access to CPNI but does not succeed at doing so, no breach has occurred. However, the

incident must be reported to NextG's CPNI Compliance Officer, who will determine whether to report the incident to law enforcement and/or take other appropriate action. NextG's CPNI Compliance Officer will determine whether it is appropriate to update NextG's CPNI policies or training materials in light of any new information. the FCC's rules require NextG on an ongoing basis to "take reasonable measures to discover and protect against activity that is indicative of pretexting."

B. Notification Procedures

As soon as practicable, and in no event later than seven (7) business days after learning of a breach, the NextG CPNI Compliance Officer shall electronically notify the United States Secret Service (USSS) and the Federal Bureau of Investigation (FBI) by accessing the following link: https://www.cpnireporting.gov. NextG's FRN number and password may be required to submit a report. If this link is not responsive, the Compliance Officer should contact counsel or the FCC's Enforcement Bureau (202-418-7450 or http://www.fcc.gov/eb/cpni) for instructions.

NextG will not under any circumstances except as provided below notify customers or disclose a breach to the public until seven (7) full business days have passed after notification to the USSS and the FBI (a full business day does not count a business day on which the notice was provided). Federal law requires compliance with this requirement even if state law requires disclosure.

If NextG receives no response from law enforcement after the seventh (7th) full business day, it must promptly proceed to inform the customers whose CPNI was disclosed of the breach. NextG will delay notification to customers or the public upon request of the FBI or USSS. If the NextG Compliance Officer believes there is a need to disclose a breach sooner, he or she should so indicate in the notification to law enforcement. However, such notification does not itself permit notice to customers; NextG still may not notify customers sooner unless given clearance to do so from both the USSS and the FBI.

IV. RECORD RETENTION

The CPNI Compliance Officer is responsible for assuring that NextG maintains for at least two years a record, electronically or in some other manner, of any breaches discovered, notifications made to the USSS and the FBI pursuant to these procedures, and notifications of breaches made to customers. The record must include, if available, dates of discovery and notification, a detailed description of the CPNI that was the subject of the breach, and the circumstances of the breach.

NextG will maintain a record of any customer complaints related to their handling of CPNI and records of NextG's handling of such complaints for at least two years. The CPNI Compliance Officer will assure that all complaints are reviewed and that NextG

considers any necessary changes to its policies or practices to address the concerns raised by such complaints.

NextG maintains a record for a period of at least one year of (1) those limited circumstances in which CPNI is disclosed or provided or made available to third parties (such release pursuant to valid request from law enforcement, the federal judiciary, or other appropriate authority); and (2) records of NextG's and its affiliates' marketing that uses CPNI, including records regarding supervisory review of marketing and of sales and marketing campaigns that use CPNI.

Because NextG does not use CPNI in any manner that would require customer approval, it does not have records associated with customers' "opt-out" approval or non-approval to use CPNI or of notification to customers prior to any solicitation for customer approval to use or disclose CPNI.

NextG will have an authorized corporate officer, as an agent of the company, sign a compliance certificate on an annual basis stating that the officer has personal knowledge that NextG has established operating procedures that are adequate to ensure its compliance with FCC's CPNI rules. The certificate for each year will be filed with the FCC Enforcement Bureau in EB Docket No. 06-36 by March 1 of the subsequent year and will be accompanied by a summary or copy of this policy that explains how NextG's operating procedures ensure that it is in compliance with the FCC's CPNI rules. In addition, the filing must include an explanation of any actions taken against data brokers and a summary of all customer complaints received in the past year concerning the unauthorized release of CPNI.

V. TRAINING

All employees with access to CPNI receive a summary of NextG's CPNI policies and are informed that (i) any use or disclosure of CPNI or other act or omission not in compliance with such policies will result in disciplinary action, including the termination of employment where appropriate, (ii) proprietary information NextG receives from another carrier for purposes of providing a telecommunications service may only be used for such purpose; and (iii) employees who knowingly facilitate the unauthorized disclosure of CPNI may be subject to criminal penalties.