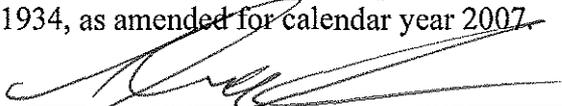


**VONAGE HOLDINGS CORP.  
SECTION 64.2009(E) CERTIFICATION  
FOR CALENDAR YEAR 2007  
EB Docket No. 06-36**

I, Louis Mamakos, a duly authorized officer of Vonage Holdings Corp., hereby certify on behalf of interconnected Voice over Internet Protocol provider Vonage America Inc. ("Vonage"), a wholly owned subsidiary of Vonage Holdings Corp., that I have personal knowledge that Vonage has established operating procedures that were adequate to ensure compliance with the rules of the Federal Communications Commission, codified at 47 C.F.R. Part 64 Subpart U, implementing Section 222 of the Communications Act of 1934, as amended.

Attached to this certification is an accompanying statement explaining how the company's procedures ensured that the company was in compliance with the rules of the Federal Communications Commission, codified at 47 C.F.R. Part 64 Subpart U, implementing Section 222 of the Communications Act of 1934, as amended for calendar year 2007.



Louis Mamakos  
Chief Technology Officer  
Vonage Holdings Corp.  
February 28, 2008

**STATEMENT REGARDING OPERATING PROCEDURES  
IMPLEMENTING 47 C.F.R. PART 64 SUBPART U  
GOVERNING USE OF  
CUSTOMER PROPRIETARY NETWORK INFORMATION (CPNI)  
FOR CALENDAR YEAR 2007**

The following statement explains how the operating procedures of Vonage America Inc., (“Vonage”), an interconnected voice over Internet protocol (“VoIP”) provider, ensured that Vonage was in compliance with the Commission’s CPNI rules, as codified at 47 C.F.R. Part 64 Subpart U, for calendar year 2007.<sup>1</sup> Except as otherwise indicated, the following applies with respect to the Commission’s rules in effect both before and after the December 8, 2007 effective date of the Commission’s April 2, 2007 Report and Order in CC Docket No. 96-115. *See* FCC 07-22 (rel. Apr. 2, 2007); Public Notice, DA 07-4915 (rel. Dec. 6, 2007).

**1. Use of customer proprietary network information without customer approval.**

Vonage used individually identifiable CPNI<sup>2</sup> for the provision of interconnected VoIP service from which the CPNI is derived, to provide customer support related to such service, and to bill and collect for such service. Vonage also used individually identifiable CPNI to protect its rights or property, or to protect users of its interconnected VoIP service and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services.

Vonage did not use or permit the use of any individually identifiable CPNI for marketing. As a result, Vonage did not use individually identifiable CPNI to market service offerings among the categories of service to which its customers already subscribed. Vonage did not use CPNI to track customers that call competing service providers.

**2. Approval required and notification for use of customer proprietary network information.**

As discussed above, Vonage used individually identifiable CPNI to provide service, to provide support to customers of its service, and to bill and collect for its service. Vonage did not use or permit the use of individually identifiable CPNI for marketing. As a result, Vonage did not make use of individually identifiable CPNI in a way that would require customer approval. Thus, it was not necessary for Vonage to provide notice to its customers about the customers’ right to restrict use of, disclosure of, and access to their individually identifiable CPNI.

**3. Safeguards required for use and disclosure of customer proprietary network information.**

*Safeguarding CPNI.* Vonage undertook technical, operational and policy measures to discover and protect against attempts to gain unauthorized access to CPNI. Specifically, Vonage

---

<sup>1</sup> Except for Vonage America Inc., none of the other subsidiaries of Vonage Holdings Corp. offered services subject to the Commission’s CPNI rules in 2007.

<sup>2</sup> In this statement, the term customer proprietary network information or CPNI means “Customer Proprietary Network Information” as that term is defined at 47 U.S.C. § 222(h)(1).

undertook a development project to update its systems to meet the Commission's new requirements for safeguarding CPNI that became effective on December 8, 2007. Vonage upgraded customer agent and account representative applications used to access CPNI while the customer is on the telephone with an agent so that the customer must provide his/her password to the agent before further access to CPNI is permitted by the system. In addition, a password is required for a customer to gain access to his/her CPNI information online. These password protections are discussed in more detail below.

Further, as part of the development project, Vonage upgraded its tracking and auditing capabilities for the systems handling CPNI. Specifically, the customer care related systems record how the customer was verified (e.g. by password or backup authentication if the customer forgot the password) for each call handled by an agent. The customer care systems also record any access by an agent to CPNI while the customer is not on the telephone and the reason why the agent accessed the CPNI. Vonage also maintains a log of changes to a customer's online or telephone account access passwords, backup authentication questions, email address, or physical address.

*Telephone access to CPNI.* As of December 8, 2007, Vonage established the use of a password as a requirement for customers to obtain access to CPNI on inbound calls. In particular, customers who purchased service over the telephone after December 8, 2007 received a personal identification number ("PIN") via email. This PIN must be used by the customer to access his/her CPNI on calls into Vonage customer care. Similarly, customers who purchased service online after December 8, 2007 were given a PIN for telephonic access to their account, as part of the subscribe process. For customers who purchased service prior to December 8, 2007 and previously were not required to use a PIN for telephonic account access, Vonage sent email messages to the customers' registered email address requesting that they set up a PIN through their online account. If an customer who purchased service prior to December 8, 2007 and had not set up a PIN through his/her online account called into customer care, the customer care representative verified the customers' identity without the use of readily available biographical information and instructed the customer to log in to his/her online account to establish a PIN and security question for backup authentication (discussed below).

After December 8, 2007, if the customer could not provide his/her PIN and could not successfully complete the backup authentication (discussed below), a Vonage customer care representative was allowed to offer to call the customer back at the phone number listed on the account to discuss the customer's CPNI. Prior to offering this call back option, however, the customer care agent was required to get approval from his/her supervisor.

In situations where the customer could not provide the correct PIN or backup authentication but was able to provide without assistance from Vonage personnel all of the call detail information necessary to address a customer care issue (i.e., the telephone number called, when it was called, and if applicable the amount charged for the call), then Vonage personnel were permitted to address that customer care issue.

*Online access to CPNI.* Vonage customers must provide a password to access CPNI online. For customers that purchased service online, establishment of a password for online access is part of the subscribe process. As of December 8, 2007, Vonage changed the password

requirements to make them more complex. Also as of December 8, 2007, for customers that subscribe over the telephone, Vonage sends a temporary password for online access to the email address provided by the customer during the subscribe process. The email message also instructs the customer to log on to his/her online account to personalize the password. If the customer does not log on to his/her online account and personalize his/her password within 7 days, Vonage sends the customer an email reminder to log on and personalize his/her password. Customers who subscribed to the Vonage service over the telephone prior to December 8, 2007 also received a temporary password for online account access. The sales agent encouraged the customer to log on to his or her online account and establish a permanent password. If these customers attempted to log on to their online account, after December 8, 2007, the system would force these customers to establish a permanent password (if they had not done so already), PIN for telephonic account access (discussed above), and security question for backup authentication (discussed below).

*Backup authentication:* As of December 8, 2007, Vonage established a backup authentication method based on a user selected security question and the customer's answer to the selected question. These questions are not based on readily available biographical information. Customers that subscribed after December 8, 2007 over the telephone receive an email message instructing them log on to their online account (see *Online Access to CPNI* above). In addition to personalizing their online password, as discussed above, when telephone subscribers log on to their account for the first time, they must select a security question and provide an answer as a backup authentication method. Customers that subscribed after December 8, 2007 online must select a security question and answer as part of the subscribe process. If a customer who purchased service prior to December 8, 2007 and had not set up a PIN and security question and answer in his/her online account called into customer care, the customer care representative verified the customers' identity without the use of readily available biographical information and instructed the customer to log in to his/her online account to establish a PIN and security question and answer for backup authentication. If an existing customer who purchased service prior to December 8, 2007 and had not set up a security question and answer in his/her online account logged on to his/her online account, the online account required that the customer select a security question and provide an answer before the customer could access the normal features of the online account.

*Notification of account changes.* As of December 8, 2007, Vonage sends email notification of account changes to customers at their email address of record. Customers receive notice for changes to their password, PIN, security questions, and E911 address.

*Training/Discipline.* Vonage has trained its employees and personnel as to when they are and are not authorized to use or access CPNI, and the Company has an express disciplinary process in place in the event CPNI policies and procedures are not followed. In this regard, as access to CPNI is considered confidential and proprietary to Vonage, it falls within the disciplinary policy of Vonage's Information Security Policy. As such, employees are subject up to, and including termination of employment or access to CPNI, if they conduct the access in a manner that is not in compliance with the FCC rules.

#### **4. Actions Against Data Brokers and Consumer Complaints**

Vonage did not take any actions against data brokers during the period covered by this statement.

Vonage did not receive any consumer complaints concerning the unauthorized release of CPNI during the period covered by this statement.