

**VONAGE HOLDINGS CORP.
SECTION 64.2009(E) CERTIFICATION
FOR CALENDAR YEAR 2013
EB Docket No. 06-36**

Annual 64.2009(e) CPNI Certification for 2014 covering the calendar year 2013

Date filed: February 28, 2014

Name of company covered by this certification: Vonage Holdings Corp.

Form 499 Filer ID: 825971 and 827095

Name of signatory: Kurt Rogers

TITLE OF SIGNATORY: Chief Legal Officer

I, Kurt Rogers, a duly authorized officer of Vonage Holdings Corp., hereby certify on behalf of interconnected Voice over Internet Protocol providers Vonage America Inc. ("Vonage") and Vonage Business Solutions, Inc. ("VBS"), both wholly owned subsidiaries of Vonage Holdings Corp., that I have personal knowledge that Vonage and VBS have established operating procedures that were 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.

Vonage and VBS have not taken any actions against data brokers in the past year. Vonage received one customer complaint in the past year concerning the unauthorized release of CPNI. VBS received no complaints in the past year concerning the unauthorized release of CPNI.

The company represents and warrants that the above certification is consistent with 47 C.F.R. § 1.17 which requires 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.



Kurt Rogers
Chief Legal Officer
Vonage Holdings Corp.
February 28, 2014

**STATEMENT REGARDING OPERATING PROCEDURES
IMPLEMENTING 47 C.F.R. PART 64 SUBPART U
GOVERNING USE OF
CUSTOMER PROPRIETARY NETWORK INFORMATION (CPNI)
FOR CALENDAR YEAR 2013**

The following statement explains how the operating procedures of Vonage America Inc. (“Vonage”) and Vonage Business Solutions, Inc. (“VBS”)¹, both interconnected voice over Internet protocol (“VoIP”) providers, ensured that they were in compliance with the Commission’s CPNI rules. *See* 47 C.F.R. § 64.2001 *et seq.*

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

As permitted by the CPNI rules,² Vonage and VBS may use CPNI without customer approval (1) to bill and collect for services rendered; (2) to protect the rights or property of Vonage and VBS, other users or other carriers from unlawful use; (3) to provide customer premises equipment and protocol conversion; (4) to provision inside wiring, maintenance and repair services; (5) to market services formerly known as adjunct-to-basic services, such as, but not limited to, speed dialing, computer-provided directory assistance, call monitoring, call tracing, call blocking, call return, repeat dialing, call tracking, call waiting, caller I.D., call forwarding and certain other Centrex features; and (6) to market services among the categories of service to which the customer already subscribes from Vonage or VBS.

Vonage and VBS used individually identifiable CPNI for the provision of service from which the CPNI is derived, to provide customer support related to such service, and to bill and collect for such service. Vonage and VBS 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. In addition, Vonage and VBS used individually identifiable CPNI to market service offerings among the categories of service to which its customers already subscribed. Vonage and VBS 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 and VBS used individually identifiable CPNI to provide service, to provide support to customers of its service, to bill and collect for its service, and to market services among the categories of service to which the customer already subscribes from Vonage or VBS. Vonage and VBS did not use or permit the use of individually identifiable CPNI for marketing outside of the categories of service to which the customer already subscribes from

¹ Vonage Holdings Corp. acquired interconnected VoIP provider Vocalocity in 2013. This transaction closed in November 2013. Vocalocity was renamed Vonage Business Solutions, Inc. and is now a wholly owned subsidiary of Vonage Holdings Corp. Vonage America, Inc., which provides Vonage interconnected VoIP services in the U.S., is also a wholly owned subsidiary of Vonage Holdings Corp.

² 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).

Vonage or VBS. As a result, Vonage and VBS did not make use of individually identifiable CPNI in a way that would require notice of such use and customer approval.

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

A. Vonage

Safeguarding CPNI. For live telephonic support, a Vonage customer must provide his/her personal identification number (“PIN”) to a Vonage agent and the agent must enter this PIN before the agent can access the customer’s CPNI in Vonage’s customer care system. In addition, a password is required for a customer to gain access to his/her CPNI information online. If the customer cannot provide his/her PIN for live telephonic support or his/her password for online account access, Vonage also has a backup authentication method. These protections are discussed in more detail below.

Additionally, 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. All customers who purchased service over the telephone 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 on the Vonage website were given a PIN for telephonic access to their account, as part of the subscription process.

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 subscription process. Customers who subscribe over the telephone are sent a temporary password for online access to the email address that was provided by the customer during the subscription 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.

Backup authentication: Vonage has established a backup authentication method based on a user selected security questions and the customer’s answer to the selected questions. These questions are not based on readily available biographical information or account information. When customers that subscribed over the telephone log on to their account for the first time, they must select their security questions and provide answers as a backup authentication method. Customers that subscribed online must select security questions and answers as part of the subscription process.

Notification of account changes. 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.

B. VBS

Online access to CPNI. VBS users must provide a password to access CPNI online. During initial user setup, a user receives a system-generated password via email for online account access. When the user first logs on the online account, the user is prompted to establish a personal password and provide answers to backup authentication questions.

The information that an individual user can view online is determined by his or her user status on the account. End Users can only view the settings and call detail records for their individual extensions. Administrators can view account payment information, past bills for the account, and call detail records for all extensions across the account. In addition, each account has one Super User. Super Users have the same access rights as Administrators but Super Users also have the ability to create or change Administrators.

Telephone access to CPNI. VBS does not provide access to call detail records over the telephone. An Administrator or Super User can request call detail records over the phone but these records will only be emailed to the current email address on file for the Super User.

Backup authentication: If the a user cannot remember his or her password, online account allows the user to receive his or her password via an email to the user's email address on file when the user is able to answers one of his or her backup authentication questions. If a user contacts VBS via telephone to resolve a password issue, care agents can reset the user's password by sending an email to the user's email address on file with a system-generated password, which restarts the process described in the *Online access to CPNI* section above.

Notification of account changes. VBS notifies users immediately via email of account changes such as password changes or address of record changes.

Training/Discipline. Vonage Business Solution's CPNI policies are included in its training materials and written policies. Any employee who improperly uses or discloses confidential business information will subject to disciplinary action, up to and including termination of employment and legal action.

4. Notification of CPNI Breaches.

Vonage and VBS have established procedures, consistent with the Commission's CPNI rules, to notify law enforcement and customers of breaches of customers' CPNI.