pillsbury

Pillsbury Winthrop Shaw Pittman LLP
2300 N Street, NW | Washington, DC 20037-1122 | tel 202.663.8000 | fax 202.663.8007

Glenn S. Richards
tel 202.663.8215
glenn.richards@pillsburylaw.com

February 29, 2012

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

Re: **EB Docket No. 06-36**
Annual 47 C.F.R. 64.2009(e) CPNI Certification for 2011

Dear Ms. Dortch:

Pursuant to Section 64.2009(e) of FCC rules, submitted herewith is RingCentral, Inc.'s 2011 CPNI certification with accompanying statement.

Should any questions arise regarding this submission, please contact the undersigned.

Sincerely yours,

Glenn S. Richards

Enclosure
cc: Best Copy and Printing, Inc.

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

EB Docket 06-36

Annual 64.2009(e) CPNI Certification for 2011

Date filed: February 24, 2012

Name of company covered by this certification: RingCentral, Inc., a California corporation

FRN: 0016-0830-40

Name of signatory: John Marlow

Title of signatory: General Counsel

I, John Marlow, certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the company 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 (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 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) against data brokers in the past year.

The company has not received any customer 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.

Signed: _____

John Marlow
General Counsel

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

EB Docket 06-36

Attachment 1: Statement Concerning Company Procedures

General duty, training, and discipline.

RingCentral, Inc. (the "Company") has adopted and distributed to all employees a CPNI policy that addresses proper handling and use of CPNI and advises all employees of their duty to safeguard CPNI. Employees are advised that violations of the confidentiality policy will subject an employee to disciplinary action, up to and including immediate termination of employment. The Company makes CPNI available to employees only on a need-to-know basis.

Use of customer proprietary network information without customer approval (47 C.F.R. § 64.2005); Approval required for use of customer proprietary network information (47 C.F.R. § 64.2007); Notice required for use of customer proprietary network information (47 C.F.R. § 64.2008); Safeguards required for use of customer proprietary network information (47 C.F.R. § 64.2009)

The Company does not use, disclose, or permit access to CPNI for marketing purposes. The Company does not disclose CPNI to third parties or permit third parties to access or use CPNI except as permitted by law.

Safeguards on the disclosure of customer proprietary network information (47 C.F.R. § 64.2010)

The Company does not provide any in-store access to CPNI.

The Company will only disclose CPNI over the telephone, based on customer initiated telephone contact, if the customer first provides a password that is not prompted a request for readily available biographical information or account information. To establish a password, the Company authenticates the customer without use of readily available biographical information or account information. Customers that have lost or forgotten their passwords may retrieve their passwords by proving an answer to a shared secret question. If a customer cannot provide the correct password or the correct response to the shared secret question, the customer must be reauthenticated and must establish a new password. In addition, customers requesting CPNI by telephone may be provided with CPNI by sending it to the customer's address of record or by calling the customer at the telephone number of record.

Customers may access their CPNI online only after they have been authenticated without using readily available biographical information or account information. After initial authentication, customers may only access CPNI online by providing a password that is not prompted by a request for readily available biographical information or account

information. Customers that have lost or forgotten their passwords may retrieve their passwords by providing an answer to a shared secret question. If a customer cannot provide the correct password or the correct response to the shared secret question, the customer must be reauthenticated and must establish a new password.

The Company notifies customers immediately by voicemail to the telephone number of record of any changes to customer password, answer to shared secret questions, online account information, or address of record. This notice does not reveal the changed information and is sent to the existing address or telephone number of record, not to an address or telephone number that has been changed.

Notification of customer proprietary information security breaches (47 C.F.R. § 64.2011)

The Company's operating procedures require notification of relevant law enforcement agencies and customers in accordance with FCC rules in the event of a breach of CPNI. The Company maintains records of any breaches discovered, notifications made to law enforcement, and notifications made to customers. These records include, where 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. The Company retains these records for 2 years.