Holland & Knight

800 17th Street, NW, Suite 1100 | Washington, DC 20006 | T 202.955.3000 | F 202.955.5564
Holland & Knight LLP | www.hklaw.com

ELECTRONIC FILING

Peter M. Connolly
202 862 5989
peter.connolly@hklaw.com

February 27, 2014

Marlene H. Dortch
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 2013
VIP Communications, Inc.

Dear Ms. Dortch:

Transmitted herewith, on behalf of VIP Communications, Inc., is its 2013 CPNI Certification and Accompanying Statement for filing in the above-referenced docket.

In the even there are any questions in connection with this filing, please communicate with the undersigned.

Very truly yours,

Peter M. Connolly

Enclosures

cc: Best Copy and Printing, Inc. via electronic mail

#11001120_v3

Annual 47 C.F.R. § 2009(e) CPNI Certification

EB Docket 06-36

Annual § 64.2009(e) Certification for 2013

Date filed: February 27, 2014

Name of company covered by this certification: VIP Communications, Inc.

Form 499 Filer ID: 821408

Name of signatory: Graham Milne

Title of signatory: President

I, Graham Milne, 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 this 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 (i.e. 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 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 _____
Graham Milne
President
VIP Communications, Inc.

VIP Communications, Inc. policy for the protection and handling of Customer Proprietary Network Information (CPNI)

1. Safeguarding CPNI

VIP Communications, Inc. (VIP) recognizes the importance and legal obligation of safeguarding CPNI information.

1.1 All customers are required to establish a customer password. Customers are also given an opportunity to setup two security questions upon logging in or calling into the customer service center if the security questions are not already setup.

1.2 If a customer fails to enter their correct password when trying to access their VIP account online, they are prompted to call customer service for assistance. Customers are also provided an option to use our password recovery system.

1.3 If they select to use the password recovery system, they are required to enter their account number or their last name and registered telephone number. They are then prompted to answer two security questions. The account password is then automatically reset to a temporary password and an email confirming the new temporary password is sent to the email address we have on record for the account.

1.4 Customers that call through the call center are authenticated by verifying there account number or phone number, their name, and providing the answer to one security question.

1.5 If the requirement in 1.4 is not met, the CSR will then ask the customer an alternative pre-established security question.

1.6 If the customer is able to satisfy the requirements of 1.5, the CSR must request a new answer to the security question that was answered incorrectly from the customer. The CSR can then continue to provide service as required to the customer.

1.7 If the customer is unable to satisfy the requirements of 1.5, the CSR will ask the customer to provide either the last number dialed or the amount and date of the first transaction on the account. If the customer successfully answers this requirement the CSR can then continue to provide service as required to the customer.

1.8 If the customer is unable to satisfy the requirements of either 1.4, 1.5 or 1.7, the customer is either sent an email to the email address on file, or a physical mail item to the delivery address on file which includes a new temporary password. The caller is only allowed limited access to add money to the account. No information from the account can be changed or released to the caller.

1.9 Under no circumstance does the CSR change the account address or any other information on the account if the requirements of either1.4, 1.5 or 1.7 are not satisfied.

1.10 VIP will generate a temporary password and mail out notice of the same to the address on the account.

2. Acceptable Use of CPNI

2.1. VIP restricts its use of CPNI for the purposes of:

a. Providing customers with account support information such as rate change information (rate change subscription).

b. Providing customers with offers and promotional information specific to their current VIP service offering (current service subscription).
c. Provide customers with offers and promotional information specific to other VIP service offerings (other service subscription)
d. Providing customers with offers and promotional information specific to products and service offerings of VIP's affiliates (affiliate promotional subscription).

2.2. VIP currently shares CPNI with its affiliate, Global Reach Communications.
2.3. All existing customers have been provided with an opt-out or opt-in notification in a form and manner appropriate with FCC regulations governing CPNI (section 64.2001 – 64.2009)
2.4. All new customers are provided with an opt-out or opt-in notification in a form and manner appropriate with FCC regulations governing CPNI (section 64.2001 – 64.2009)
2.5. VIP maintains a complete record for a minimum of one year of all marketing campaigns for which CPNI is used.
2.6. VIP maintains a complete record for a minimum of one year of all disclosures or provisions of CPNI to any third party.
2.7. All use of CPNI, whether internal or external, must receive supervisory review and approval from a VIP Vice President or higher. A record of such reviews is maintained for a period of at least one year.

3. Customer Subscription Options (Opt-in and Opt-out)

3.1. VIP provides every customer with the option to opt-out of all email subscription services when opening a new VIP account.
3.2. VIP provides a click through link on every email sent that allows a customer to opt-out of any subscription.
3.3. Customers can opt-out of any subscription service by logging into their VIP account online or by calling the VIP customer service center.
3.4. Customer can opt-in to any subscription service by logging into their VIP account online. Customers cannot opt-in by calling VIP customer service.
3.5. VIP maintains a record of all changes to a customer's subscriptions for a period of at least one year. Such records included the date and time of the change and the method of the change (online or through customer service).

4. Employee Training and Disciplinary Procedures

4.1. VIP ensures that all employees who have access to CPNI are trained on the procedures laid out in this policy document.
4.2. VIP will issue a written warning to any employee who breaches these procedures. If an employee breaches these policies a second time, their employment with VIP will be terminated.

5. Actions in the Case of a Breach in CPNI Procedures

5.1. In the case of breach of these CPNI procedures, VIP will firstly act to protect against continued breach.

5.2. VIP will notify law enforcement of any breach as soon as possible but not later than seven business days following the breach.

5.3. Unless otherwise directed by the relevant investigating agency, VIP will not notify customers or any other party of the breach until seven business days have elapsed following the notification to law enforcement.

5.4. Records of all breaches will be maintained by VIP for a minimum of two years.