neptuno
SEAMLESS
TECHNOLOGY
SOLUTIONS

NeptunoMedia, Inc.
Statement of CPNI Compliance for 2018

NeptunoMedia, Inc. ("Neptuno" or the "Company") provides this statement to the Federal Communications Commission' ("FCC" or the "Commission") pursuant to 47 C.F.R. § 64.2009(e) of the Commission's rules regarding customer proprietary network information ("CPNI"). As explained below and as stated in the attached certification by Carlos M. Figueroa Domínguez, Neptuno is in compliance with the Commission's CPNI rules, as set forth at 47 C.F.R. §§ 64.2001, *et seq*. Neptuno obtains CPNI as a provider of interconnected VoIP services to enterprise customers in Puerto Rico.

Neptuno uses, discloses, and permits access to CPNI in accordance with the Commission's rules. Neptuno does not use CPNI for marketing its services, does not share CPNI with its affiliates or any data brokers, and does not use CPNI to identify or track customers that call competing service providers. Neptuno only shares CPNI with certain third parties contracted by Neptuno for the limited purposes of providing customer service support, to properly authenticate a customer's identity, or to validate a customer's consent to any changes in service.

Prior to commencing employment with Neptuno, all employees execute a Confidentiality Agreement, pursuant to which the employee is precluded from accessing and using CPNI in a manner that is inconsistent with the FCC's CPNI rules. A representative from the Company's Human Resources department ensures that the employee adequately understands the restrictions regarding to use, disclosure, and protection of CPNI collected by the Company, and that the agreement is executed with the employee's understanding. The originally executed Confidentiality Agreement is kept and maintained with the employee's file at Neptuno's offices.

Because Neptuno does not use any CPNI for marketing purposes, it does not maintain a record of the sales and marketing campaigns that use CPNI.

Neptuno has adopted a policy that substantially limits the extent to which CPNI is available to its employees. The provisioning system, which contains CPNI, is only accessible by personnel in Neptuno's provisioning and network operations center ("NOC") departments, which currently consists of only 20 employees. Each employee has his or her own unique login and access credentials.

Any customer requesting CPNI from Neptuno must be previously authenticated by providing the Company with confidential information that is contained in the customer's underlying service agreement. If the customer cannot do so, it must provide Neptuno with written proof of its identity to obtain access to the requested CPNI. Upon a change in the authentication information, Neptuno places a telephone call to the authorized customer contact set forth on the service agreement, and follows up with an email to the customer, to which the customer must reply with confirmation of the change in authentication information. If the customer does not have a known email address, Neptuno places a fax to the customer, to which the customer must respond with confirmation.

neptuno
SEAMLESS
TECHNOLOGY
SOLUTIONS

In the event of an unauthorized disclosure of CPNI, the Company is authorized to take the necessary measures to investigate the violation and take all remedial and disciplinary action in accordance with the Company's policies. As of the date of this filing, Neptuno has not discovered or received notice of any actual or alleged unauthorized disclosures of CPNI.

Upon the discovery of a data breach in which CPNI was exposed or accessed, Neptuno commences a thorough internal and external investigation to determine the source and cause of the breach. No later than seven business days after learning of the breach, Neptuno electronically notifies the Federal Bureau of Investigation (FBI) and United States Secret Service (USSS) of the breach through the online reporting facility. No earlier than seven business days after notifying the FBI and USSS, Neptuno informs the customers affected by the CPNI breach, providing each such customer with the dates of discovery and notification, a detailed description of the CPNI that was subject to the breach, and the circumstances of the breach. Notification is sent to each affected customer via fax and electronic mail (if that information is on record), followed by a phone call to the authorized contact listed on each customer's respective contract documentation. Neptuno retains all CPNI breach information for a period of 2 years.

Certification

I, Carlos M. Figueroa Domínguez, Data Center Director/Security Officer of Neptuno, duly authorized to submit this Certification on behalf of NeptunoMedia, Inc., hereby declare under penalty of perjury that, to the best of my knowledge, information, and belief, the foregoing is true and correct.

Carlos M. Figueroa — Name

2-27-19 — Date

P. O. Box 191995, San Juan, PR 00919-1995
Tel: (787) 774-0018 Fax: (787) 775-0081 info@neptunopr.com