Annual 47 C.F.R. § 64.2010 CPNI Certification

EB Docket No. 06-36

Annual 64.2010(e) CPNI Certification for 2017

Name of company covered by this certification: Proximiti Technologies, Inc. d/b/a Proximiti Communications, Inc., Proximiti Mobility, Inc., Proximiti Mobility, LLC, and SipStorm, Inc.

Date Filed: February 20, 2018

Filer IDs: 826647 and 829879

Name of Signatory: Donald C. Davis

Title of Signatory: Chief Financial Officer

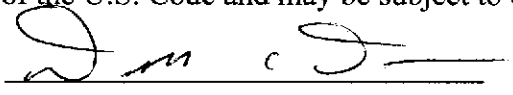
I, Donald C. Davis, certify that I am an officer of Proximiti Technologies, Inc. d/b/a Proximiti Communications, Inc. Proximiti Mobility, Inc., Proximity Mobility, LLC, and SipStorm, Inc. ("Proximiti") and acting as an agent of Proximiti, that I have personal knowledge that the company has operating procedures and policies in place that are designed to ensure compliance with the Federal Communications Commission's ("Commission") 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 are designed to maintain compliance with the Commission's CPNI rules.

Proximiti has not taken any actions (proceedings instituted or petitions filed by a company at either state commissions, the court system, or the Commission) against data brokers in the past year. Proximiti did not receive any complaints during the 2017 calendar year concerning the unauthorized release of CPNI.

Proximiti has taken measure to protect against attempts to gain unauthorized access to CPNI. Proximiti has not discovered any information about the processes that pretexters are using to attempt to gain access to CPNI other than the information that already is contained publicly in this docket. As mentioned in Attachment A, Proximiti has implemented CPNI safeguards, including, but not limited to, maintaining customer verification processes and applying role-based authorization (limiting employees with access to data on a need-to-know basis).

Proximiti 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. Proximiti also acknowledges that false statements and misrepresentations to the Commission are punishable under Title 18 of the U.S. Code and may be subject to enforcement action.

Signed: 

Date: February 20, 2018

ATTACHMENT A

PROXIMITI TECHNOLOGIES, INC. d/b/a PROXIMITI COMMUNICATIONS, INC., PROXIMITI MOBILITY, INC., PROXIMITI MOBILITY, LLC AND SIPSTORM, INC.

STATEMENT OF CPNI OPERATING PROCEDURES

Proximiti Technologies, Inc. d/b/a Proximiti Communications, Inc., Proximiti Mobility, Inc., Proximity Mobility, LLC, and SipStorm, Inc. (in aggregate "Proximiti") is a national reseller of interexchange services, an interconnected Voice over Internet Protocol ("VoIP") provider doing business in Florida and a provider of wireless services in Texas. Proximiti is Florida owned and operated and provides high-quality voice and enhanced services to approximately three hundred business customers.

Proximiti has established policies and procedures that are designed to ensure that it is in compliance with the Federal Communications Commission's ("Commission") rules regarding the use, disclosure, and access to CPNI. Proximiti provides this statement pursuant to Section 64.2010(e) of the Commission rules, 47 C.F.R. § 64.2010(e), to summarize those procedures and policies.

PERMISSIBLE USES OF CPNI

Proximiti limits its use of CPNI unless necessary. Proximiti may use, disclose, or permit access to CPNI for the following purposes: (1) to initiate, provision, render, and bill and collect for the telecommunications services from which such information is derived; (2) to provide the services necessary to, or used in, the provision of the VoIP services that Proximiti provides, including in the publishing of directories; (3) to protect our rights and property, or to protect our customers and other carriers from fraudulent, abusive or unlawful use of, or subscription to, our services. We also may use CPNI to provide any inbound telemarketing, referral, or administrative services to the customer for the duration of the call, if the customer initiated the call and approves the use of such information to provide services. Proximiti has implemented protections to protect against unauthorized disclosure or access to CPNI in the limited instances where it is required to share or disclose CPNI with third parties, such as for billing and collection.

USE OF CPNI FOR MARKETING PURPOSES

Currently, Proximiti does not use CPNI to conduct outbound marketing or in connection with its sales and marketing campaigns. In the event that Proximiti does use CPNI for marketing purposes, it will fully comply with the applicable Commission rules.

EMPLOYEE TRAINING/DISCIPLINARY PROCESS:

Proximiti trains its personnel as to what information is classified as CPNI and when they are authorized and not authorized to use this information. Proximiti has an express disciplinary process for the misuse and/or mishandling of customer information including CPNI, which includes the potential for termination.

DATA SECURITY BREACHES/REQUESTS FOR CPNI

Proximiti will notify the United States Secret Service and the Federal Bureau of Investigation in the event of a data breach. Unless law enforcement directs otherwise, we will notify affected customers of the breach as soon as practicable after the expiration of the seven business day waiting period. We will maintain a record in accordance with section 64.2011(d) of any breaches discovered, notifications made to law enforcement, and notifications made to customers for at least two years.

Proximiti also has procedures in place for responding to requests for CPNI from any person other than the customer. It is Proximiti's policy not to release any information to any person other than the customer's authorized representative absent a validly issued subpoena.

CUSTOMER COMPLAINTS

Proximiti has procedures in place to track any complaints it receives concerning the unauthorized use, disclosure, or access to CPNI. If we receive complaints regarding CPNI, we will break them down by category, and provide a summary of the complaints in the annual certification that we submit to the Commission.

CPNI SAFEGUARDS

Proximiti utilizes authentication procedures for in-coming calls, customer-service representative initiated inquiries, and online account access. All online accounts are password protected, and Proximiti establishes those passwords without the use of readily available biographical information or account information. Proximiti also has implemented procedures to address lost or stolen passwords. These procedures do not rely on the use of readily available biographical information or account information.

Proximiti prohibits its employees from releasing call detail information to any customer during an in-bound call. Proximiti employees may provide call detail information by sending it to the customer's address of record or by calling the customer at his/her telephone number of record.

Proximiti employees are required to be mindful of any attempts to compromise customer CPNI, including, but not limited to, any actions that pretexters may be taking to gain access to CPNI.

Proximiti also has implemented network security measures including implementing role-based security measures, pursuant to which personnel have access only to information that is necessary for their particular position. To this end, few individuals within Proximiti have full range of access to CPNI.

NOTIFICATION OF ACCOUNT CHANGES

Proximiti notifies its customers immediately, via email, of certain account changes including any changes in the customer's online password, a change in the customer's address of record, a change in the customer's online account, and a change of the back-up means of authentication for lost or stolen passwords.