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

**EB Docket 06-36**

Annual 64.2009(e) CPNI Certification for 2015 covering calendar year 2014

Date filed: February 20, 2015

Name of companies covered by this certification:

| | |
|---|---|
| ExteNet Systems, Inc. | 827267 |
| ExteNet Systems (California), LLC | 827267 |
| ExteNet Systems (Virginia), LLC | 827267 |
| ESI Advanced Wireless Networks, LLC | 828275 |

Name of signatory: George A. Vinyard

Title of signatory: VP, General Counsel, Secretary

I, George A. Vinyard, certify that I am an officer of the companies named above, and acting as an agent of the companies, that I have personal knowledge that the companies have 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, consisting of the CPNI Compliance Policies and Operating Procedures of ExteNet Systems, Inc., ExteNet Systems (California), LLC, ExteNet Systems (Virginia), LLC, and ESI Advanced Wireless Networks, LLC that describes the steps taken to protect CPNI and explains how the companies' procedures ensure that they are in compliance with the requirements set forth in section 64.2001 *et seq.* of the Commission's rules.

The companies have not taken any actions against data brokers in the past year.

The companies have not received any customer complaints in the past year concerning the unauthorized release of CPNI.

Signed _____

George A. Vinyard
Vice President
ExteNet Systems, Inc.
ExteNet Systems (California) LLC
ExteNet Systems (Virginia) LLC
ESI Advanced Wireless Networks, LLC

---

**Attachments:** Accompanying statement explaining CPNI procedures.

## CPNI Compliance Policies and Operating Procedures of ExteNet Systems Inc.

ExteNet Systems, Inc., ExteNet Systems (California) LLC, and ExteNet Systems (Virginia) LLC, and ESI Advanced Wireless Networks, LLC (collectively "ExteNet") have the following policies and procedures to protect the confidentiality of Customer Proprietary Network Information ("CPNI") pursuant to the Federal Communications Commission ("FCC") rules set forth in 47 C.F.R. Part 64, Subpart U, sections 2001 *et seq* implementing section 222(c) of the Communications Act of 1934, as amended. ExteNet's policies are administered by George Vinyard, ExteNet's CPNI Compliance Officer.

CPNI is defined as "(A) information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and (B) information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier; except that such term does not include subscriber list information." 47 U.S.C. § 222(h)(1).

ExteNet is a carrier's carrier whose customers are wireless service providers with their own end user customers ("Carrier Customer(s)"). ExteNet executes a specific nondisclosure agreement with each of its Carrier Customers that protects the confidentiality of the Carrier Customer's information. ExteNet does not have any access to the CPNI of its Carrier Customers' own customers. ExteNet leases or licenses telecommunications infrastructure for use by its Carrier Customers and has only limited access to certain CPNI of its Carrier Customers. ExteNet has developed policies and operating procedures designed to protect such CPNI from data brokers, pretexters, or any other type of unauthorized access, as outlined below in detail.

# I. Use, Disclosure, and Access to CPNI

In accordance with 47 U.S.C. § 222(c) and 47 C.F.R. §§ 64.2001 *et seq*, ExteNet has implemented policies and operating procedures to allow disclosures of CPNI only where permitted.

### A. Use of CPNI without Customer Approval

ExteNet may use, disclose, or permit access to CPNI, without customer approval, for: billing and collection; administrative customer care services; maintenance and repair services; to protect its rights or property; to protect its customers and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, its services; responding to a lawful law enforcement request for such information; or use of aggregate customer information. With respect to third party vendors, including those providing inside wiring installation, maintenance, and repair services on ExteNet's behalf, such vendors are subject to nondisclosure agreements with respect to any CPNI they may obtain. ExteNet does not use CPNI for marketing purposes at this time.

### B. Use of CPNI with Customer Approval

ExteNet does not currently use CPNI in a manner that requires prior customer approval. Should ExteNet change this policy, ExteNet would seek approval from and give notice of rights to its Carrier Customers pursuant to 47 C.F.R. §§ 64.2007–64.2008 for any use, disclosure or access to CPNI requiring customer approval. As required, ExteNet's CPNI Compliance Officer would maintain records of all notifications and requests for approvals.

## II. Safeguards against Unauthorized Use or Disclosure of or Access to CPNI to Unauthorized Parties

In accordance with 47 U.S.C. § 222(c) and 47 C.F.R. §§ 64.2001 *et seq*, ExteNet has policies and operating procedures to safeguard against any unauthorized use or disclosure of CPNI to unauthorized parties. Additionally, ExteNet has nondisclosure agreements in place to protect its Carrier Customers' confidential information.

### A. Safeguards on Use, Disclosure of or Access to CPNI

Pursuant to 47 C.F.R. § 64.2009, ExteNet has implemented a system to safeguard against any unauthorized use, disclosure of or access to CPNI. ExteNet does not currently use, disclose, or permit access to CPNI for marketing. Any contemplated use, disclosure of or access to CPNI for marketing purposes will require senior management review and, if approved, ExteNet will implement any necessary safeguards as required under the FCC's rules.

#### 1. Training

As required by 47 C.F.R. § 64.2009(b), ExteNet trains all employees regarding the CPNI policies and operating procedures. The training program outlines when the employees are or are not authorized to use, disclose or permit access to CPNI and the disciplinary process if CPNI policies and/or operating procedures are violated, up to and including termination of employment.

ExteNet trains its employees to identify a "breach" as defined in the FCC's rules. ExteNet instructs its employees to contact ExteNet's CPNI Compliance Officer and email cpni@extenetsystems.com if they become aware of, suspect or attempt any breaches of CPNI. The CPNI Compliance Officer will determine if a breach has occurred and take appropriate steps pursuant to 47 C.F.R. § 64.2011 and ExteNet's internal policy and operating procedures on reporting CPNI breaches to law enforcement.

It is ExteNet's policy that all employees report any suspected breach regardless of external or internal origin, including the employee's own actions. Employees that fail to report an intentional or unintentional breach caused by their own actions will be disciplined more severely than employees who come forward immediately.

#### 2. CPNI Compliance Officer

As required by 47 C.F.R. § 64.2009(e), ExteNet appointed George A. Vinyard, VP, General Counsel, and Secretary of ExteNet Systems, Inc. as the CPNI Compliance Officer for ExteNet, including ExteNet Systems (California) LLC, ExteNet Systems (Virginia) and ESI Advanced Wireless Networks, LLC.. The CPNI Compliance Officer is responsible for filing ExteNet's annual CPNI compliance certifications, maintaining records regarding CPNI, and monitoring and enforcing ExteNet's policies and operating procedures internally.

The CPNI Compliance Officer is responsible for making any reports to the FCC if opt-out mechanisms do not work property pursuant to 47 C.F.R. § 64.2009(f) or any reports of breach of CPNI to the United States Secret Service and Federal Bureau of Investigation pursuant to 47 C.F.R. § 64.2011.

The CPNI Compliance Officer maintains for at least two (2) years a record of any disclosures, notices to customers regarding rights, suspected breaches, reported breaches, and any and all other information related to CPNI and the enforcement of these policies and operating procedures. The CPNI Compliance Officer will also revise and update these policies and operating procedures as needed to address any concerns that arise in their application.

### B. Safeguards on Disclosure of CPNI

In order to discover and protect against attempts to gain unauthorized access to CPNI and pursuant to 47 C.F.R. § 64.2010, ExteNet has implemented a system to detect and protect against any unauthorized disclosure of CPNI.

In addition to ExteNet's policies and operating procedure, all electronic formats of CPNI are protected using best security practices. ExteNet's servers are stored in a locked room within ExteNet's larger office. Additionally, ExteNet limits internal access to CPNI to select employees based upon specific need to access CPNI. These select employees may only access CPNI after providing their proper login and password, which must be changed periodically for greater protection.

ExteNet physically secures CPNI in a room with an electronic lock or within locking filing cabinets. During normal business hours, an ExteNet employee is stationed inside the front entrance and only unsecured entrance into the office. Outside of normal business hours, ExteNet's office is secured by an electronic lock and an alarm system.

#### 1. Telephone Access to CPNI

As required by 47 C.F.R. § 64.2010(b), ExteNet authenticates its Carrier Customers without the use of readily available biographical information or account information when a Carrier Customer initiates telephone contact. While ExteNet does not have access to call detail information, a proper password pursuant to 47 C.F.R. 64.2010(e) is nonetheless required before ExteNet discloses any CPNI to a Carrier Customer via telephone.

If a Carrier Customer cannot be authenticated or provide the correct password, ExteNet calls the Carrier Customer at the telephone number of record or provides the information by mail via the address of record.

#### 2. Online Access to CPNI

In accordance with 47 C.F.R § 64.2010(c), ExteNet allows its Carrier Customers to access CPNI online through a system that requires authentication and a password. If any account information, including password, backup authentication method, online account or address of record is changed, ExteNet notifies its Carrier Customers that there has been a change without revealing the changed information pursuant to 47 C.F.R 64.2010(f).

All of ExteNet's Carrier Customers are business customers, and the business customer exemption set forth in 47 C.F.R. § 64.2010(g) applies to the extent ExteNet and its Carrier Customers have contractual provisions in place governing customer authentication.

ExteNet does not have any retail stores, so the requirements set forth in 47 C.F.R. § 64.2010(d) are not applicable.

## III. Reporting CPNI Breaches to Law Enforcement

In accordance with 47 C.F.R. § 64.2011, ExteNet has implemented policies and operating procedures governing reporting CPNI breaches to law enforcement. Any ExteNet employee that becomes aware of, suspects or attempts any breaches of CPNI must report such information to ExteNet's CPNI Compliance Officer immediately. No reports or disclosures will be made to the customer except as allowed under 47 C.F.R. § 64.2011(b)-(c).

Upon learning of a breach, ExteNet will notify the United Secret Services and Federal Bureau of Investigation using the link: http://www.fcc.gov/eb/cpni. In no event will this notification be later than seven (7) business days after a reasonable determination of the breach. If ExteNet believes there is an extraordinary urgent need to notify its Carrier Customer, it shall indicate this in its notification. ExteNet shall cooperate with the investigating agency, including not notifying the customer if instructed by the investigating agency.

If ExteNet does not receive instruction from law enforcement after seven (7) business days of its report, it will notify its Carrier Customer of the breach. ExteNet follows state law customer notification requirements to the extent state law is not inconsistent with 47 C.F.R. § 64.2011.

ExteNet's CPNI Compliance Officer is responsible for maintain a record for two (2) years of any breaches and subsequent notifications made to law enforcement. These records shall include the "dates of discovery and notification, a detailed description of the CPNI that was subject of the breach, and the circumstances of the breach." 47 C.F.R. § 64.2011(d).