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

EB Docket 06-36

Annual 64.2009(e) CPNI Certification for 2018 covering the prior calendar year 2017

Date: February 27, 2018

Name of company covered by this certification: Millennium Telcom, LLC d/b/a OneSource Communications

Form 499 Filer ID: 820278

Name of signatory: Garrick Whitnah

Title of signatory: VP of Finance

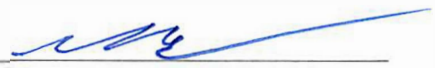
I, Garrick Whitnah, certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the Company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. *See* 47 C.F.R. § 64.2001 *et 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, safeguards, 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 is not aware of any attempts by pretexters to access the CPNI of the Company's customers and has not had to take any actions against data brokers.

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 

Attachment: Accompanying Statement explaining CPNI procedures

ACCOMPANYING STATEMENT

This statement explains how Millennium Telcom, LLC d/b/a OneSource Communications ("the Company") procedures ensure compliance with the FCC's rules on CPNI and the safeguarding of such customer information.

The Company has a written CPNI policy that explains what CPNI is, when it may be used without customer approval, and when customer approval is required prior to CPNI being used, disclosed or accessed for marketing purposes.

The Company has assigned a Director for CPNI Compliance to serve as the central point of contact regarding the Company's CPNI responsibilities and questions related to CPNI policy. The Director for CPNI Compliance has responsibilities including, but not limited to, supervising the training of all Company employees with access to CPNI, investigating complaints of unauthorized release of CPNI, and reporting any breaches to the appropriate law enforcement agencies. The Director for CPNI Compliance also maintains records in accordance with FCC CPNI rules, including records of any discovered breaches, notifications of breaches to law enforcement, and law enforcements' responses to the notifications, for a period of at least two years.

The Company has internal procedures in place to educate its employees about CPNI and the disclosure of CPNI. Employees with access to this information are aware of the FCC's rules and are prohibited from disclosing or permitting access to CPNI without the appropriate customer consent. Employee disclosure of CPNI is only as allowed by law and the FCC rules. In accordance with Company policy, any employee that uses, discloses, or permits access to CPNI in violation of Federal regulations is subject to disciplinary action, and possible termination.

The Company requires express opt-in consent from a customer prior to the release of CPNI to a joint venture partner or independent contractor for marketing purposes.

Appropriate safeguards on the disclosure of CPNI have been implemented in accordance with C.F.R. §64.2010. Prior to the disclosure of CPNI, customers initiating calls to or visiting the Company's offices are properly authenticated. Passwords and password back-up authentication procedures for lost or forgotten passwords are implemented in accordance with §64.2010(e). For a new customer, the Company requests that the customer establish a password at the time of service initiation. For existing customers to establish a password, the Company must first authenticate the customer without the use of readily available biographical information or account information. The Company authenticates a customer by

calling the customer back at their telephone number of record or reviewing a valid, photo ID that matches information on the account, if the customer is in a retail office.

Call detail information is only disclosed over the telephone, based on customer-initiated telephone contact, if the customer first provides a password that is not prompted by the carrier asking for readily available biographical information or account information. If the customer does not provide a password, call detail information is only provided by sending it to the customer's address of record or by calling the customer at their telephone number of record. If the customer is able to provide call detail information to the Company during a customer-initiated call without the Company's assistance, then the Company is permitted to discuss the call detail information provided by the customer. Prior to the Company disclosing CPNI to a customer visiting any of its retail offices in person, the customer must present a valid photo ID matching the customer's account information.

The Company does not rely on readily available biographical information or account information to authenticate a customer's identity before a customer can access CPNI online. Once authenticated, a customer cannot access his or her telecommunications account without a password that is not prompted by the Company asking for readily available biographical information or account information.

The Company has implemented procedures to notify customers immediately whenever a password, customer response to a back-up means of authentication for lost or forgotten passwords, or address of record is created or changed.

The Company has established procedures, and trained employees responsible for obtaining customer authorization to use CPNI for marketing purposes, regarding the notice and approval requirements under §64.2008. The Company has complied with the notice requirements for Opt-Out.

The Company has developed and utilizes a system for maintaining readily accessible records of whether and how a customer has responded to Opt-Out approval as required by §64.2009(a).

The Company maintains a record of sales and marketing campaigns that use our customers' CPNI. The Company shall maintain a record of all instances where CPNI was disclosed or provided to third parties, or where third parties were allowed access to CPNI. Records are retained for a minimum of one year.

The Company has established a supervisory review process regarding its compliance with the rules for outbound marketing situations. Prior to any outbound marketing effort, sales personnel must obtain supervisory approval of any proposed

marketing request for customer approval. The Company maintains records of its compliance for a minimum of one year.

In the event of a CPNI breach, the Company complies with the FCC's rules regarding notice to law enforcement (i.e, United States Secret Service (USSS) and the Federal Bureau of Investigation (FBI)) and customers. Records of any CPNI breach and notifications to law enforcement, as well as law enforcement's responses are maintained for a period of at least two years.