



February 29, 2008  
*Via ECFS Transmission*

2600 Maitland Center Pkwy.  
Suite 300  
Maitland, FL 32751  
P.O. Drawer 200  
Winter Park, FL  
32790-0200  
Tel: 407-740-8575  
Fax: 407-740-0613  
www.tminc.com

Marlene H. Dortch, Commission Secretary  
Office of the Secretary  
Federal Communications Commission  
445 – 12<sup>th</sup> Street, SW – Suite TW-A325  
Washington, D.C. 20554

**RE: EB Docket No. 06-36 CPNI Certification for U.S. Metropolitan Telecom, LLC  
d/b/a Truwave Networks LLC**

Dear Ms. Dortch:

In accordance with Federal Communications Commission's Public Notice of January 29, 2008, and pursuant to 47 C.F.R. § 64.2009(e), U.S. Metropolitan Telecom, LLC d/b/a Truwave Networks LLC hereby files its Certification of Customer Proprietary Network information (CPNI) for the year 2007 and supporting Statement. As directed by the Public Notice, please include this Certification in EB Docket No. 06-36.

Please contact me at 407-740-3031 or [sthomas@tminc.com](mailto:sthomas@tminc.com) if you have any questions about this filing.

Sincerely,

Sharon Thomas  
Consultant to  
U.S. Metropolitan Telecom, LLC  
d/b/a Truwave Networks LLC

*ST/im.*  
*Enclosure*

Copy: Enforcement Bureau (*provided via ECFS website*)

Best Copy and Printing (*FCC@BCPIWEB.COM*)

TMS: FCX0801  
File: Metropolitan Telecom – FCC Certs / Orders

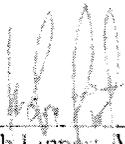
ANNUAL 47 C.F.R. § 64.2009(e) OFFICER'S CERTIFICATION OF  
CUSTOMER PROPRIETARY NETWORK INFORMATION (CPNI) COMPLIANCE

EB Docket 06-36

Annual 64.2009(e) CPNI Certification for Calendar Year: 2007  
Name of company covered by this certification: U.S. Metropolitan Telecom, LLC d/b/a  
Truwave Networks LLC  
Form 499 Filer ID: 826718  
Name of signatory: Josh Lippert  
Title of signatory: VP Finance

I, Josh Lippert, certify and state that:

1. I am the Vice President of Finance of U.S. Metropolitan Telecom, LLC d/b/a Truwave Networks LLC ("Truwave") and, acting as an agent of the company, I have personal knowledge of Truwave's operating procedures as they relate to CPNI, and the Rules and Regulations of the Federal Communications Commission regarding CPNI.
2. I hereby certify that, to the best of my knowledge, information and belief, Truwave's operating procedures are adequate to ensure compliance with its CPNI obligations pursuant to Section 222 of the Communications Act of 1934, as amended, and the Commission's rules found at 47 CFR Subpart U.
3. Attached to this certification as Exhibit A is an accompanying statement explaining how the company's procedures ensure that the company is in compliance with the requirements set forth in section 64.2001 *et seq.* of the Commission's rules.

  
\_\_\_\_\_  
Josh Lippert, VP Finance

  
\_\_\_\_\_  
Date

**Exhibit A**  
**Statement of CPNI Procedures and Compliance**

## **U.S. Metropolitan Telecom, LLC d/b/a Truwave Networks LLC**

### **Statement of CPNI Procedures and Compliance**

U.S. Metropolitan Telecom, LLC d/b/a Truwave Networks LLC (“Truwave” or “the Company”) does not use or permit access to CPNI to market any services outside of the total service approach as specified in 47 CFR §64.2005. If Truwave elects to use CPNI in a manner that does require customer approval, it will follow the applicable rules set forth in 47 CFR Subpart U, including the institution of operational procedures to ensure that notification is provided and customer approval is obtained before CPNI is used or disclosed.

The Company trains its employees as to when they are and are not authorized to use CPNI. Employees receive this training during their new employee initiation and in annual refresher training. Truwave has a strict disciplinary process in place for the unauthorized use or improper disclosure of CPNI, which includes dismissal of employees who violate the Company policy.

Truwave maintains a record of all sales and marketing campaigns that use CPNI. All outgoing marketing campaigns are reviewed and must be approved by a supervisor who is knowledgeable regarding CPNI requirements prior to initiation of the campaign. The Company also maintains a record of all instances where CPNI was disclosed or provided to third parties, or where third parties were allowed access to CPNI.

Truwave has processes in place to safeguard its customers' CPNI from improper use or disclosure by employees and to discover and protect against attempts by third parties to gain unauthorized access to customer CPNI. Specifically, the Company has stringent network security in place which restricts access to customer data at multiple levels. Passwords are issued to employees based on need, which allow access only to the specific levels of information that the employee requires to perform his/her job responsibilities. Data access audit trails are maintained so that the Company can track access into the secure systems and determine if improper access has occurred.

Company does not disclose CPNI over the telephone in response to a customer-initiated telephone inquiry, unless the customer can provide the call detail information that is the subject of the inquiry without the assistance of a customer service representative. If it elects to do so in the future, it will follow the applicable rules set forth in 47 CFR Subpart U, including the implementation of authentication procedures that do not require the use of readily available biographical information or account information and customer notification of account changes.

Truwave has instituted authentication procedures to safeguard the disclosure of CPNI online. These procedures do not require the use of readily available biographical information or account information as defined by the FCC. The company authenticates customers at the time of service initiation when the customer executes a service contract

and establishes a password for online access. Passwords do not rely on readily available biographical information or account information. Unless the appropriate password is provided, Truwave does not allow on-line access to CPNI.

The Company does not offer a back-up authentication method.

Truwave immediately notifies customers whenever a password, online account, or address of record is created or changed without revealing the changed information or sending the notification to the new account information.

Truwave does not have any retail locations and therefore does not disclose CPNI in-store.

Truwave has put in place procedures to notify law enforcement in the event of a breach of customers' CPNI and to ensure that customers are not notified of the breach before the time period set forth in the FCC's rules, or, if applicable, when so authorized by law enforcement. While the Company has not had any breaches to report, it has a process in place to maintain records of all breaches discovered and notifications made to the USSS and the FBI, and to customers.

The Company has not taken any actions against data brokers in the last year.

Truwave did not receive any customer complaints about the unauthorized release of CPNI or the unauthorized disclosure of CPNI in calendar year 2007.

The Company has not developed any information with respect to the processes pretexters are using to attempt to access CPNI.

---