Annual 47 C.F.R. § 64.2009(e) CPNI Certification
EB Docket 06-36

Marlene H. Dortch
Office of the Secretary
Federal Communications Commission
445 12th Street, SW, Suite TW-A325
Washington, DC 20554

Annual 64.2009(e) CPNI Certification for 2014

Filing Period: March 1, 2015

Name of company covered by this certification: Midstate Communications, Inc.

Form 499 Filer ID: 803454

Name of signatory: Ryan Wilhelmi

Title of signatory: President

I, Ryan Wilhelmi, 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*.

Statement of Compliance with CPNI Rules: Our Company's procedures ensure compliance with the requirements set forth in section 64.2001 *et seq.* of the Commission's rules. See the attached statement for a discussion of our CPNI compliance efforts.

Companies must report on any information that they have with respect to the processes pretexters are using to attempt to access CPNI , and what steps companies are taking to protect CPNI. Our Company has not taken any actions (proceedings instituted or petitions filed by a company at either state commissions, the court system, or at the Commission) against data brokers in the past year.

No pretexters have attempted to access our CPNI.

The company has not received any customer complaints in the past year concerning the unauthorized release of CPNI

Signed

Ryan Wilhelmi

Statement Regarding CPNI Rule Compliance

The operating procedures of Filer ensure that the company complies with Part 64, section 2001 et.seq. of the FCC rules governing the use of CPNI.

Filer has adopted a CPNI procedure manual which is required reading for all employees which have access to CPNI. The CPNI procedure manual provides that CPNI information is not to be released to any person except in accordance with the steps outlined in the CPNI procedure manual. The CPNI manual further provides that violation of CPNI polices will result in disciplinary action which could include employment termination. Our company has designated a CPNI compliance officer who periodically reviews CPNI compliance rules with persons who have access to CPNI. The CPNI procedure manual is approximately twenty-six (26) pages long and would be provided to the Commission upon request. Filer would prefer to keep the CPNI procedure manual as confidential as a safeguard against review by pretexters.

Filer has established a system by which the status of a customer's approval for the use of CPNI can be clearly established prior to the use of CPNI. For telephone or online CPNI access these procedures include the use of passwords/PINs established after the identity of the caller has been verified; the use of mail delivered to the customer's address of record; and/or a call by our company to the number of record and subsequent identity verification via account specific information contained on the last company bill (such as amount due, amount of last payment, or other non-public account information). For retail location CPNI access we require a valid photo ID (a government-issued personal identification such as a driver's license or passport, or comparable ID) which matches the name on the account. The Company relies on the involvement of its supervisory/management to ensure that use of CPNI complies with applicable rules and law.

Filer's procedure is that a customer is notified immediately when a password, customer response to a back-up authentication means for lost/forgotten passwords, online account, or address of record is created or changed.

Filer's procedure requires that customers opt-in before CPNI is used by third parties to market services. However, at this time, our company does not utilize CPNI in marketing campaigns.

Filer's procedure is that within seven (7) days of discovery of an unauthorized release of CPNI we send an electronic notice to the United States Secret Service (USSS) and the Federal Bureau of Investigation (FBI). Unless either of these agencies requests that we postpone notifying the subscriber, the subscriber will be notified about the unauthorized release of CPNI within seven (7) days after law enforcement notification. In exceptional cases we will notify the law enforcement agencies of our desire to notify more promptly the subscriber about an unauthorized CPNI disclosure. Filer maintains a log of unauthorized use of CPNI. Upon occurrence of a CPNI breach the log will include the date of discovery, notification to law enforcement, description of the breach, circumstances of the breach and a supervisor's signature and date. This log is maintained for a minimum of two years.