

Attachment 1

Statement attached to made part of the Annual 47 C.F.R. §64.2009(e) CPNI Certification

CPNI Procedures

OPEN Mobile is a provider of Commercial Mobile Radio Service ("CMRS") and does not offer telecommunications service to its customers in categories other than CMRS. OPEN Mobile does not currently use customer proprietary network information ("CPNI") for the purpose of marketing services other than CMRS, customer premises equipment, and information services to its customers. Nor does OPEN Mobile share CPNI with third parties, unless requested by duly authorized law enforcement officials. Consequently, OPEN Mobile is not required to maintain either an "opt-in" or "opt-out" system with respect to CPNI. In the event that OPEN Mobile were to change the ways in which it uses CPNI, any such change would be reviewed and approved by the company's Chief Operations Officer, who is familiar with the FCC's rules governing the use of CPNI and who is the certifying officer for CPNI purposes.

OPEN Mobile has established procedures to protect its customers sensitive information. OPEN Mobile maintains all CPNI on a secure server, and CPNI is only accessible through a custom reporting tool available only to specially-trained employees at corporate headquarters and in the field. Open Mobile has established procedures to ensure employees with access to CPNI handle this information properly and according to the FCC's CPNI rules. All employees with access to CPNI are trained on what constitutes authorized versus non-authorized CPNI disclosure. Procedures in place include express disciplinary actions for the unauthorized use of CPNI.

OPEN Mobile offers two different services to customers, each of which requires a distinct approach to the application of CPNI requirements. One service model offers service to customers

via a prepaid billing similar to that of MetroPCS (representing over 99 percent of OPEN Mobile's customer base), while the other service model offers service to customers via a traditional postpaid billing (representing the remaining customers, who account for less than 1 percent of its customer base).

OPEN Mobile does not offer its prepaid customers the ability to access call detail information by telephone or over the Internet. Call detail information is released to prepaid customers only by presenting a written request in person, including the presentation of valid identification and the customer password. However, the company allows for a limited exception to these procedures in connection with the release of CPNI to law enforcement personnel only upon presentation of a valid subpoena or court order. OPEN Mobile provides non-call detail related CPNI to its prepaid customers via the Internet only after the customer provides a valid user ID and password.

For the small percentage of OPEN Mobile's customers subscribed to postpaid service, OPEN Mobile provides call detail CPNI only in the following circumstances: (1) an in-person request with the presentation of valid identification; (2) a request via the Internet and the customer's provision of the correct password; or (3) a request by telephone, in which case the records are mailed to the customer's mailing address of record. In the event that a subscriber requesting CPNI over the Internet cannot supply a valid password, CPNI will be released only upon the presentation of unique identifying information establishing that the requesting party is, in fact, the subscriber whose records are requested. In such circumstances, a customer's online password is reset by e-mail confirmation to the customer's e-mail address of record. However, the company allows for a limited exception to these procedures in connection with the release of CPNI to law enforcement personnel only upon presentation of a valid subpoena or court order.

Attachment 2

Statement attached to made part of the Annual 47 C.F.R. §64.2009(e) CPNI Certification

Summary of Customer Complaints

Customer complaints in the past year concerning the unauthorized release of CPNI:

- Case # 1: Customer # 1103376 claimed on June 13, 2011 that a company employee disclosed information related to calls and text messages to a third party. An investigation was conducted but no unauthorized disclosure of information was identified with respect to the customer account. Consequently, the company determined that no unauthorized release of CPNI data had occurred. The customer was notified of the investigation results and was given a briefing regarding company security procedures regarding call details and other CPNI.
- Case # 2: Customer # 1800878 claimed on April 19, 2011 that a company employee disclosed his account personal information to a third party. An investigation was conducted and the unauthorized disclosure of information was confirmed. Consequently, the company disciplinary actions were applied and the employee resigned his employment. The customer was notified of the investigation results and was given a briefing regarding company security procedures regarding call details and other CPNI.