

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

EB Docket 06-36

Annual 64.2009(e) CPNI Certification for 2008

Date filed: June 16, 2008¹

Name of company covered by this certification: PRWireless, Inc. d/b/a OPEN Mobile

Form 499 Filer ID: 826742

Name of signatory: Federico Grosso

Title of signatory: VP-Finance

I, Federico Grosso, certify that I am an officer of PRWireless, Inc. d/b/a OPEN Mobile ("OPEN Mobile"), and acting as an agent of OPEN Mobile, that I have personal knowledge that OPEN Mobile 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 procedures of OPEN Mobile ensure that OPEN Mobile is in compliance with the requirements set forth in section 64.2001 *et seq.* of the Commission's rules.

OPEN Mobile 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) against data brokers in the past year.

OPEN Mobile has not received any customer complaints in the past year concerning the unauthorized release of CPNI.

Signed _____


¹ OPEN Mobile first came into existence on June 22, 2007, on which date it acquired the FCC licenses formerly held by NewComm Wireless Services, Inc. As described in the attached statement, OPEN Mobile has established procedures for the protection of CPNI but inadvertently failed to file this certification when due as the result of an oversight. OPEN Mobile and its counsel have taken steps to ensure that its future CPNI certifications are filed in a timely manner.

Statement

OPEN Mobile is a provider of Commercial Mobile Radio Service (“CMRS”) and does not offer telecommunications services 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 affiliates or with third parties, other than pursuant to requests 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 VP-Finance, 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 maintain the security of CPNI of its customers. For example, OPEN Mobile maintains all CPNI on a secure server, and CPNI is accessible only through a custom reporting tool available to specially-trained employees at corporate headquarters and in the field. At the present time, OPEN Mobile has two separate processes concerning the disclosure of CPNI, one covering its customers who receive service via a prepaid model similar to that of MetroPCS (representing approximately 90 percent of its customer base) and the other covering its customers who receive traditional postpaid services (representing the remaining customers, who account for roughly 10 percent of its customer base).

OPEN Mobile does not release call detail CPNI relating to its prepaid customers by telephone, by Internet, or in person except to law enforcement personnel upon presentation of a valid subpoena or court order. OPEN Mobile releases non-call detail CPNI to its prepaid customers via the Internet only after the customer provides a valid user ID and password.

For the relatively small percentage of OPEN Mobile’s customers who subscribe to postpaid service, OPEN Mobile releases call detail CPNI to customers in the following circumstances: (1) an in-person request and 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 a customer's address of record. In the event that a subscriber requesting CPNI by 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.