

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

EB Docket 06-36

Annual 64.2009(e) CPNI Certification for 2013

Date filed: March 1, 2013

Names and Form 499 Filer IDs of companies covered by this certification¹:

MetroPCS California, LLC	821528
MetroPCS Florida, LLC	825836
MetroPCS Georgia, LLC	821526
MetroPCS Michigan, Inc.	825647
MetroPCS Texas, LLC	825648
MetroPCS Nevada, LLC	827147
MetroPCS Pennsylvania, LLC	827149
MetroPCS New York, LLC	827563
MetroPCS Massachusetts, LLC	827560
MetroPCS Networks, LLC	825871

Name of signatory: Roger D. Linquist

Title of signatory: Chairman & CEO

I, Roger D. Linquist, certify that I am an officer of the companies named above (collectively, "MetroPCS"), and acting as an agent of MetroPCS, that I have personal knowledge that MetroPCS 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 operating procedures of MetroPCS ensure that MetroPCS is and remains in compliance with the requirements set forth in section 64.2001 *et seq.* of the Commission's rules.

MetroPCS 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.

¹ This certification also covers, to the extent required, the following MetroPCS affiliates not listed above: MetroPCS Wireless, Inc., which holds an international Section 214 authorization issued by the Commission but does not have its own Form 499 Filer ID because it provides service through the subsidiaries listed herein; and MetroPCS AWS, LLC, MetroPCS 700 MHz, LLC, MetroPCS Networks California, LLC and MetroPCS Networks Florida, LLC, each of which holds licenses issued by the Commission but has no customers and no Form 499 Filer ID. If and when these entities begin serving customers, their customers' CPNI will be handled in accordance with the same operating procedures described in the accompanying statement.

Except as listed below, MetroPCS has received no customer complaints in the past year concerning the unauthorized release of CPNI:

- Customer A complained that Customer A's account was accessed by a third party who cancelled two lines of service on Customer A's account and changed the calling plan on the remaining two lines. Upon investigation, MetroPCS determined that the third party was an Authorized User who had presented the proper password for the account prior to making the changes. At the request of Customer A, MetroPCS reactivated the two disconnected lines and returned the two remaining lines to the prior calling plan, and considers the matter to be closed.
- Customer B complained that unauthorized changes were made by a third party to service plans on and that new phones were activated on Customer B's account. MetroPCS determined that the changes were made by a third party Authorized User possessing Customer B's correct PIN, enabling that third party to make changes. Customer B returned to a MetroPCS store with the original phones that were on the account, and MetroPCS placed the original phones back on the account at Customer B's request. MetroPCS also placed the Customer B's account on high security at Customer B's request, and considers the matter to be closed.

Signed: /s/ Roger D. Linquist

Statement

MetroPCS is a provider of Commercial Mobile Radio Service (“CMRS”). MetroPCS does not currently use customer proprietary network information (“CPNI”) for the purpose of marketing services in categories other than those to which the customer already subscribes and with respect to CMRS services to market customer premises equipment and information services related to its CMRS services (collectively, “CMRS-Related Services”) to its customers. Except as allowed under the Commission’s rules, MetroPCS does not disclose CPNI to, or permit access to CPNI by, third parties. MetroPCS does not to maintain either an “opt-in” or “opt-out” system with respect to CPNI because, among other things, (1) MetroPCS markets services to customers in categories of service to which the customer already subscribes; (2) any use of CPNI for the marketing of services outside the categories of service to which the customer already subscribes is done pursuant to 47 C.F.R. § 64.2008(f); and (3) MetroPCS only discloses CPNI to law enforcement officials pursuant to subpoenas or other lawful process with which MetroPCS believes in good faith it is obligated to comply. While not having a need to do so, MetroPCS voluntarily offers its customers the ability to opt out of marketing messages relating to CMRS-Related Services sent by MetroPCS. In the event that MetroPCS were to change how it uses CPNI, any such change would be reviewed and approved by MetroPCS’ CEO, who is familiar with the FCC’s rules governing the use of CPNI and who is the certifying officer for CPNI purposes.

MetroPCS has established procedures to maintain the security of CPNI of its customers. For example, MetroPCS maintains all CPNI on an a third-party billing provider server and CPNI relating to call detail is accessible only through a reporting tool available to MetroPCS employees at corporate headquarters and in the field. MetroPCS has a confidentiality agreement with such third-party billing provider that limits its ability to use or disclose MetroPCS’ customers’ CPNI. Further, MetroPCS requires that each customer establish a unique, secure password upon service activation, and releases non-call detail CPNI by telephone only to a subscriber upon the subscriber’s provision of the correct password. In the event that a subscriber cannot supply a valid password, non-call detail 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. Additionally, MetroPCS releases call detail records to customers only upon an in-person request and presentation of valid identification. If a customer’s identification does not match the records of MetroPCS (for example, in the case of a customer whose handset is provided by his or her employer), then a person in the store will place a call to the handset in order to verify the customer’s identity.