



February 6, 2006

Electronic Filing

Ms. Marlene H. Dortch
Secretary
Federal Communications Commission
445 12th Street, SW
Room TW-A325
Washington, DC 20554

Re: Certification of CPNI Filing February 6, 2006
EB Docket No. 06-36
File No. EB-06-TC-060

Dear Ms. Dortch:

Pursuant to Section 64.2009(e) of the Commission's Rules, 47 C.F.R. § 64.2009(e), and the Commission's public notice released February 2, 2006 regarding the above proceedings, attached please find T-Mobile USA, Inc.'s most recent CPNI certification and accompanying statement. If you have any questions regarding this filing, please contact the undersigned.

Sincerely,

/s/ David A. Miller
David A. Miller
Sr. Vice President & General Counsel
T-Mobile USA, Inc.

Attachment

cc: Byron McCoy, Telecommunications Consumers Division, Enforcement Bureau, FCC
Best Copy and Printing, Inc.

Main: 202-654-5900
Fax: 202-654-5963
401 9th Street NW, Suite 550
Washington, DC 20004

CPNI Compliance Certificate and Statement

This CPNI Compliance Certificate and Statement is prepared pursuant to Section 64.2009(e) of the Federal Communications Commission's rules and regulations, 47 C.F.R. § 64.2001 et seq.

On behalf of T-Mobile USA, Inc. ("T-Mobile" or "Company"), I, David A. Miller, an officer of T-Mobile, certify that to the best of my personal knowledge, based on personal information and inquiry, the following is true:

T-Mobile has in place the operating procedures and systems summarized in the following statement to safeguard customer proprietary network information ("CPNI") from improper use and disclosure.

Access -

T-Mobile has implemented procedures and systems that contain safeguards to protect, and restrict access to, customer information. Such procedures and systems include:

Upon hire, all new employees, including Company Customer Care representatives and Retail Store representatives, are required to sign confidentiality agreements which specifically cover customer information; the Company employee handbook reiterates T-Mobile employee confidentiality obligations with respect to such customer information; and Company Customer Care and Retail Store representatives are provided with reminders relating to the confidentiality and protection of customer information.

Customer information is contained in T-Mobile's billing and operations systems. T-Mobile restricts access to these systems to those employees needing access to perform their job functions. Access is based on individual login IDs and passwords. Levels of access to systems and customer information vary, and are determined by the employee's job function.

Workstations and applications used by Company Customer Care employees contain safeguards to protect customer information, including as described below:

Core Company Customer Care systems (as with other T-Mobile systems that permit access to customer information) require that users have a unique user ID and password. Company Customer Care systems automatically require that passwords be changed regularly. System access to Company Customer Care systems is denied after repeated log in attempts are made with incorrect passwords.

Company Customer Care representatives may only access approved websites. In addition, logs are created to track access to websites, which allow for monitoring of such activity. Company Customer Care workstations do not have floppy disk drives or CD Rom drives.

The “run” function on Company Customer Care workstations is disabled to prevent downloading and installation of unauthorized applications. Applications are delivered to workstation desktops according to assigned individual user profiles. Company Customer Care representatives are not permitted to alter their desktops. Company Customer Care systems create audit logs of access to customer information performed by the Customer Care representative; this log is stamped with the name of the Customer Care representative who initiated the transaction.

Employee Training –

Company Customer Care representatives receive six weeks of rigorous training, which includes training regarding Company policies on the use and confidentiality of customer information. Representatives must achieve a 90% or higher examination score to become a Company Customer Care representative. The Company periodically provides ongoing, mandatory training to all Company Customer Care representatives. Such training also covers protecting the confidentiality of customer information. Completion of the training is monitored and tracked by the Company. All live Company Customer Care calls are recorded, and a subset of those calls are assessed for quality and compliance with Company policies. An employee’s failure to follow policies or procedures will result in corrective action, up to and including termination. Company Customer Care systems automatically identify and stamp when a customer account is accessed, or modified by a Customer Care representative.

Upon hire, Retail Store Representatives receive approximately 40 hours of training, including live training, and on-line training which is tracked with automated training software. The training includes, training on safe-keeping of customer information, Company policies including confidentiality of customer information, and Company policy that breach of such confidentiality policies will result in disciplinary action, up to and including termination. Retail Store Representatives are tested at the end of such training and are required to achieve at least an 85% examination score.

Employee Discipline Program -

Any employee found to have violated T-Mobile’s policies, including those concerning the protection of customer information, is subject to disciplinary action, up to and including termination.

Review Process and System For Record Retention for Marketing Campaigns -

T-Mobile tracks and records the Company’s customer marketing campaigns via a campaign management system. Dedicated Company legal counsel or outside legal counsel are responsible for review of marketing campaigns.

Process to Maintain Customer Approvals -

T-Mobile currently does not share CPNI with third parties for their marketing purposes wherein customer notice and record-keeping may be applicable. Appropriate customer notice and record-keeping practices will be put in place if T-Mobile decides in the future to share CPNI for such purposes.

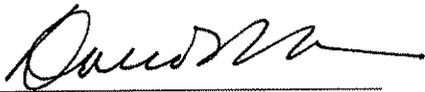
Method To Ensure That T-Mobile Sends Opt-Out Notifications -

T-Mobile currently does not share CPNI with third parties for their marketing purposes wherein a customer opt-out or opt-in notice may be applicable. Nonetheless, T-Mobile does maintain an opt-out database for customers allowing a customer to opt-out of marketing campaigns conducted by T-Mobile.

Organization -

T-Mobile has a chief Privacy Officer and a Director of Information Security Policy and Compliance with responsibility for Company policies regarding customer information. T-Mobile also has an Information Security and Privacy ("IS&P") Council that includes the Chief Financial Officer, Chief Marketing Officer, Chief Information Officer, Senior VP Product Development & Engineering, Senior VP Customer Care, Senior VP Sales, Senior VP General Counsel, VP-General Manager HotSpots, and the VP of Risk Management & Assurance. The IS&P Council provides direction and guidance regarding the Company's information security and privacy functions, including the protection of customer information. Supervisory personnel throughout T-Mobile are responsible for enforcing Company policies regarding customer information.

Dated: January 26, 2006



David A. Miller
Senior Vice President & General Counsel
T-Mobile USA, Inc.