Annual 47 C.F.R. § 64.2009(e) Customer Proprietary Network Information ("CPNI") Certification for the period from January 1, 2008 to December 31, 2008
EB Docket 06-36

Date Filed:	**February 24, 2009**
Name of company covered by this certification:	**T-Mobile USA, Inc. ("T-Mobile")**
Form 499 Filer ID:	**822060** (T-Mobile USA, Inc.) **817978** (SunCom Wireless Operating Company, LLC) **825855** (T-Mobile Puerto Rico LLC)
Name of Signatory:	**David A. Miller**
Title of Signatory:	**Senior Vice President & General Counsel**

I, David A. Miller, certify that I am an officer of the company named above, that I am acting as an agent of the company, and that, to the best of my personal knowledge, based on personal information and inquiry, the company has established operating procedures designed to ensure compliance with the Commission's CPNI rules contained in 47 C.F.R. §§ 64.2001 *et seq*.

Attached to this certification is an accompanying "Statement Regarding T-Mobile USA, Inc. Customer Proprietary Network Information Operating Procedures" explaining how the company's procedures during the certification period were designed to ensure that the company is in compliance with the requirements set forth in section 64.2001 *et seq*. of the Commission's rules.

The company has not taken any actions against data brokers in the past year. Neither has the company become aware of any new or novel processes used by pretexters. Moreover, as explained in the accompanying statement, the company has taken numerous steps to protect CPNI.

The company has received customer complaints during the certification period concerning the unauthorized release of CPNI. A summary of all such complaints during the certification period is included as an attachment to the accompanying statement – see Attachment A.

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

STATEMENT REGARDING T-MOBILE USA, INC.

CUSTOMER PROPRIETARY NETWORK INFORMATION ("CPNI")

OPERATING PROCEDURES

T-Mobile USA, Inc. ("T-Mobile" or "Company") provides this statement pursuant to 47 C.F.R. § 64.2009(e) to explain how T-Mobile's operating procedures were designed to ensure compliance with the Federal Communications Commission's ("Commission") CPNI rules for the period from January 1, 2008 to December 31, 2008. This statement also covers the 2008 operations of two indirectly wholly owned subsidiaries of T-Mobile USA, Inc. – SunCom Wireless Operating Company, LLC (referred to herein as "T-Mobile Carolinas") and T-Mobile Puerto Rico LLC (referred to herein as "T-Mobile Puerto Rico"), acquired by T-Mobile from SunCom Wireless, Inc. effective February 22, 2008. Although T-Mobile continues to report operations for these subsidiaries through separate Form 499 IDs, the process of integrating and re-branding their operations, including the conversion to T-Mobile's data systems, policies, and procedures, was substantially completed as of September 2008. Where the policies or procedures for those subsidiaries materially differed from those of T-Mobile during any portion of the statement period, those differences are described herein.

Certification

T-Mobile requires an officer of the Company to sign and file with the Commission a compliance certification on an annual basis. The certification is made to the best of the personal knowledge of the certifying officer, based on personal information and inquiry, that T-Mobile has established operating procedures designed to ensure compliance with the Commission's CPNI rules. T-Mobile's certifying officer relies in substantial part upon sub-certifications of corporate officers and managers directly responsible for implementing the Company's CPNI operating procedures.

Customer Approval to Use, Disclose, or Permit Access to CPNI

T-Mobile's policy is not to use, disclose, or permit access to its customers' CPNI except as such use, disclosure, or access is permitted without customer approval, or as otherwise provided in Section 222 of the Communications Act of 1934, as amended. Accordingly, the customer notice and associated record-keeping requirements of the Commission's CPNI rules are not applicable. Should T-Mobile change its policies such that the use, disclosure, or permitted access to CPNI requires customer approval, appropriate customer notice, record-keeping, and Commission notification practices will be implemented.

Consistent with the Commission's rules, although T-Mobile does not necessarily engage in each of the following activities, T-Mobile's policies permit it to use, disclose, or permit access to CPNI without customer approval for the purpose of:

- providing or marketing service offerings among the categories of service (*i.e.,* Commercial Mobile Radio Service ("CMRS")) to which the customer already subscribes;

- provisioning Customer Premises Equipment ("CPE") and information service(s);

- conducting research on the health effects of CMRS;

- marketing services formerly known as adjunct-to-basic services, such as, but not limited to, speed dialing, computer-provided directory assistance, call monitoring, call tracing, call blocking, call return, repeat dialing, call tracking, call waiting, caller I.D., call forwarding, and certain centrex features;

- protecting the rights or property of the carrier, or protecting users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services; and

- as otherwise permitted in Section 222 of the Communications Act of 1934, as amended.

Notice of CPNI Rights

As explained above, T-Mobile's policy is not to use, disclose, or permit access to its customers' CPNI except as permitted without customer approval, or as otherwise provided in Section 222 of the Communications Act of 1934, as amended. Therefore, T-Mobile is not required to provide customer notice regarding CPNI rights as prescribed in the Commission's rules. Should T-Mobile change its policies such that customer notice is required, such notice will be provided. T-Mobile does inform its customers through its online Privacy Policy that under federal law, the customer has a right, and T-Mobile has a duty, to protect the confidentiality of CPNI and that consistent with this duty, T-Mobile's policies permit disclosure of CPNI only as required or as permitted by law.

Record Retention for Marketing Campaigns

T-Mobile's policy is to maintain records of sales and marketing campaigns that use CPNI. Records include a description of each campaign, the specific CPNI that was used in the campaign, and what products and services were offered as a part of the campaign. T-Mobile maintains such records for at least one year.

Reporting Opt Out Failures

T-Mobile's policy is not to use, disclose, or permit access to its customers' CPNI except as permitted without customer approval under the Commission's rules or as otherwise provided in Section 222 of the Communications Act of 1934, as amended. Should T-Mobile change its policies and seek customer approval to use, disclose, or permit access to CPNI, T-Mobile will provide written notice of opt-out failures to the Commission within five business days as specified in the Commission's rules.

Supervisory Review Process

T-Mobile has a supervisory review process regarding compliance with the CPNI rules for its outbound marketing campaigns. T-Mobile has dedicated in-house legal counsel responsible for the review of marketing campaigns.

Safeguarding CPNI

T-Mobile takes the privacy and security of CPNI seriously and has implemented reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI. In addition to its internal policies, which are designed to ensure compliance with the Commission's CPNI Rules, T-Mobile publishes an online Privacy Policy for its customers, which explains how T-Mobile uses, discloses, and protects customer information, including CPNI, consistent with applicable law.

General Privacy and Security Measures

T-Mobile has implemented numerous controls designed to ensure compliance with the Commission's CPNI rules. For example, T-Mobile has an Information Security and Privacy ("IS&P") Council, which provides governance and oversight regarding the Company's information security and privacy functions, including the safeguarding of CPNI. The Council includes several T-Mobile senior executives. Similarly, T-Mobile has dedicated several employees to work exclusively on privacy and security issues. For example, T-Mobile has a Vice President of Risk Management & Assurance, a Principal Privacy Officer, and a Senior Manager of Enterprise Information Technology Security. T-Mobile's Risk Management and Assurance organization is responsible, among other things, for ensuring that T-Mobile's security policies and practices are adequate and forward-looking. T-Mobile's Principal Privacy Officer's organization is responsible, among other things, for ensuring that T-Mobile develops, maintains, and follows adequate privacy policies, practices, and procedures related to the protection of customer information, including CPNI. T-Mobile's Enterprise Information Technology Security organization is responsible for ensuring that data security policies and practices are implemented and monitored. Under the oversight of the IS&P Council, these executives and their respective staffs, along with other T-Mobile employees tasked with specific privacy and security responsibilities within other T-Mobile organizations, work with

employees across the company to implement T-Mobile's privacy and security policies designed to protect customer information, including CPNI.

T-Mobile also has implemented comprehensive methods and procedures governing the handling of CPNI, and has developed extensive information system controls and requirements related to the storage and handling of such data. T-Mobile conducts internal reviews and audits that evaluate the security of customer data.

Customer Authentication Procedures

T-Mobile has established procedures that require proper authentication prior to disclosing CPNI based on customer-initiated telephone contacts, in-store visits, and online. With the exception of T-Mobile Puerto Rico, T-Mobile's policy is not to disclose call detail information over the telephone in response to customer-initiated telephone contacts.[1] T-Mobile Puerto Rico may disclose call detail over the telephone in response to a customer-initiated telephone contact, but its policy allows such disclosure only after verifying the customer's account password *and* verifying a one-time use Personal Identification Number or "PIN" sent to the customer's handset during the call. T-Mobile has also implemented procedures designed to ensure that bill reprints are only sent to an address of record on file for at least 30 days.[2]

T-Mobile's policy is to require a valid government-issued photo ID matching the customer's account information prior to disclosing CPNI during a visit to a retail store.[3] T-Mobile's policy is to permit online account access to CPNI only with a password – initially established through use of a randomly-generated PIN delivered to the customer by means of a Short Message Service ("SMS") text message to the telephone number of record. T-Mobile also allows customers the option to establish account passwords for use outside the online environment (e.g., for calls to customer care) but requires the customer requesting such a password to authenticate without the use of readily available biographical information or account information (i.e., through the use of a randomly-generated PIN delivered to the customer by means of an SMS text message to the

---

1 Until June 2008, T-Mobile Carolinas released call details if requested during a customer-initiated telephone contact, but only pursuant to a separate outbound call placed by the customer service representative to a customer telephone number of record.

2 T-Mobile Puerto Rico did not implement such procedure to ensure that bill reprints were only sent to an address of record on file for at least 30 days until August 2008.

3 T-Mobile utilizes a customer-established PIN for authentication of pre-paid accounts at retail locations (as well as for calls to customer care). Unlike with post-paid and "contract" customers, T-Mobile does not collect from pre-paid customers identification sufficient information to authenticate the customer by photo ID on subsequent store visits.

telephone number of record).[4] T-Mobile Puerto Rico utilizes a mandatory password authentication for calls to customer care.

Employee & Representative Training Program

T-Mobile provides Company-wide training to educate its employees and representatives regarding the confidentiality of customer information, including authorized and unauthorized uses of CPNI. T-Mobile augments this Company-wide training with targeted training for Customer Care and Retail Sales Representatives. Such training provides front-line employees and representatives with additional information concerning safeguarding CPNI and other customer information along with specific training regarding proper authentication of inbound customer inquiries by telephone, online, or in retail stores. T-Mobile further augments the Company-wide CPNI training by providing additional training to specific functional groups, such as the marketing and legal departments. All T-Mobile employees are also required to sign confidentiality agreements that specifically cover the handling of customer information, including CPNI.

Employee Discipline Program

T-Mobile has an express disciplinary process in place to address noncompliance with Company policies, including policies concerning employee use of, access to, and disclosure of CPNI. An employee found to have violated T-Mobile's policies, including policies relating to use of, access to, and disclosure of CPNI, is subject to disciplinary action up to and including termination.

Notice of Account Changes

T-Mobile's policy is to mail a notice to the customer's address of record or send an SMS message to the customer's number of record within one business day whenever, among other changes, a password, customer response to a back-up means of authentication for lost or forgotten passwords, online account, or address of record is created or changed.[5] T-Mobile's policy is that any notice sent to an address of record is sent only to an address associated with the customer's account for at least 30 days (except for accounts activated within the last 30 days, in which case the notice is sent to the

---

[4] Until September 2008, T-Mobile Carolinas and T-Mobile Puerto Rico did not require the customer requesting to establish a customer care password to authenticate without the use of readily available biographical information or account information. However, as explained above, neither T-Mobile Carolinas nor T-Mobile Puerto Rico released call details in response to customer-initiated calls based solely on password authentication.

[5] Until September 2008, T-Mobile Carolinas and T-Mobile Puerto Rico prepared and mailed account change notices on Mondays, Wednesdays, and Fridays – generally resulting in such notices being sent within 48 hours.

address provided at account activation). Any such notice does not include or reveal the changed information.[6]

Notice of Security Breaches

T-Mobile's policy is to notify law enforcement as soon as practicable, but in no event later than seven (7) business days, after a reasonable determination has been made that a breach of its customer's CPNI has occurred. The notice process conforms to procedures established by the Commission and is otherwise in accordance with 47 C.F.R. § 64.2011.

T-Mobile's policy is to notify customers of the breach no sooner than the eighth business day following completion of the notice to law enforcement unless directed by the U.S. Secret Service or the FBI not to so disclose or notify customers. T-Mobile respects any agency request that T-Mobile not to disclose the breach for an initial period of up to 30 days, which may be extended further by the agency. The requesting agency must provide its direction in writing, as well as any notice that delay is no longer required.

Recordkeeping of Unauthorized Disclosures of CPNI, Customer Complaints, and Actions Taken Against Pretexting

T-Mobile's policy is to maintain a record of CPNI security breaches, notifications made to law enforcement, and notifications made to customers for at least two years.

T-Mobile's policy is that customer complaints concerning the unauthorized release of CPNI are reported and investigated internally, and are broken out by category of complaint (e.g., instances of improper access by employees, instances of improper disclosure to individuals not authorized to receive the information, or instances of improper access to online information by individuals not authorized). A summary of all such complaints during the certification period is included along with the annual certification to the Commission – attached hereto as Attachment A.

A record of any actions taken by T-Mobile against data brokers is maintained and an explanation of such actions included with the annual certification to the Commission, including any information T-Mobile has with respect to new or novel processes or schemes pretexters are using to attempt to access CPNI. T-Mobile is committed to constant assessment and improvements in its security and operating procedures with respect to CPNI.

---

[6] Until September 2008, T-Mobile Carolinas and T-Mobile Puerto Rico did not provide customer notices regarding the establishment of or change to customer care passwords (notices were provided for online passwords). As noted in footnote 4, however, T-Mobile Carolinas and T-Mobile Puerto Rico did not disclose call detail information over the phone based solely on customer care password authentication.

ATTACHMENT A

SUMMARY OF T-MOBILE USA, INC. CUSTOMER COMPLAINTS CONCERNING THE ALLEGED UNAUTHORIZED RELEASE OF CPNI

T-Mobile has implemented comprehensive policies and procedures to capture (and investigate) all customer complaints made to any company business channel (*e.g.*, customer care, retail, Web, etc.) concerning alleged unauthorized release of CPNI. For the period from January 1, 2008 to December 31, 2008, T-Mobile received complaints by category, and after investigation confirmed breaches as a result of such complaints, as follows:

	Complaints Received	Confirmed Breaches
Alleged Improper Access by T-Mobile Employees	48	9
Alleged Improper Disclosure to Other Unauthorized Persons	578	49
Alleged Improper Online Access by Unauthorized Persons	59	1
Total	685	59