

MOBILE COMMUNICATIONS TECHNOLOGY INC.

945 North Peerless Road
Evansville, IN 47712
Phone: 812-424-5140
Fax: 812-424-5172

Marlene H. Dortch, Office of the Secretary
Federal Communications Commission
445 12th Street, SW
Washington, D.C. 20554

Re: **Annual 47 C.F.R. § 64.2009(c) CPNI Certification for 2007
EB Docket No. 06-36**

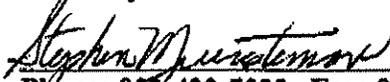
Form 499 Filer ID: 821792

CERTIFICATION

I, Stephen Muensterman, secretary/treasurer for Mobile Communications Technology, Inc. (MCTI) hereby certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures effective immediately that are adequate to ensure compliance with the Customer Proprietary Network Information rules set forth in 47 C.F.R. §§ 64.2001 *et seq.* of the rules of the Federal Communications Commission.

Attached to this certification is an accompanying statement that (i) explains how the company's procedures ensure that the company is in compliance with the requirements set forth in 47 C.F.R. §§ 64.2001 *et seq.* of the rules, (ii) explains any actions taken against data brokers during the past year, (iii) summarizes all customer complaints received in the past year concerning the unauthorized release of CPNI and (iv) reports information known to the company regarding tactics pretexters may be using to attempt access to CPNI.

Stephen Muensterman
Secretary/Treasurer for Mobile Communications Technology (MCTI)

 Date: 9-11-2008
Phone: 812-423-7322 Fax: 812-423-9099

Carrier: Mobile Communications Technology Inc.
Address: 945 North Peerless Road
Evansville, Indiana 47712-2933

STATEMENT

Carrier has established operating procedures that ensure compliance with the Federal Communication Commission ("Commission") regulations regarding the protection of customer proprietary network information ("CPNI").

- Carrier has implemented a system whereby the status of a customer's CPNI approval can be determined prior to the use of CPNI.
- Carrier continually educates and trains its employees regarding the appropriate use of CPNI. Carrier has established disciplinary procedures should an employee violate the CPNI procedures established by Carrier.
- Carrier maintains a record of its and its affiliates' sales and marketing campaigns that use its customers' CPNI. Carrier also maintains a record of any and all instances where CPNI was disclosed or provided to third parties, or where third parties were allowed access to CPNI. The record includes 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.
- Carrier has established a supervisory review process regarding compliance with the CPNI rules with respect to outbound marketing situations and maintains records of carrier compliance for a minimum period of one year. Specifically, Carrier's sales personnel obtain supervisory approval of any proposed outbound marketing request for customer approval regarding its CPNI, and a process ensures that opt-out elections are recorded and followed.
- Carrier took the following actions against data brokers in 2007, including proceedings instituted or petitions filed by Carrier at a state commission, in the court system, or at the Federal Communications Commission: **None Taken**

- Carrier has established procedures to ensure that customers will be immediately notified of account changes including changes to passwords, back-up means of authentication for lost or forgotten passwords, or address of record.
- The following is a summary of all customer complaints received in 2007 regarding the unauthorized release of CPNI:
 - Number of customer complaints Carrier received in 2007 related to unauthorized access to CPNI, or unauthorized disclosure of CPNI: **No Complaints Received**
 - Category of complaint:
 - __0__ Number of instances of improper access by employees
 - __0__ Number of instances of improper disclosure to individuals not authorized to receive the information
 - __0__ Number of instances of improper access to online information by individuals not authorized to view the information
 - __0__ Number of other instances of improper access or disclosure
 - Description of instances of customer complaints, improper access or disclosure:
No Complaints or Improper Access

Mobile Communications Technology Inc.
CUSTOMER PROPRIETARY NETWORK INFORMATION (“CPNI”)
POLICIES AND PROCEDURES

I. Statement of Corporate Policy

The policy of **Mobile Communications Technology Inc. (MCTI)** is to comply with the laws of the United States pertaining to Customer Proprietary Network Information (“CPNI”) contained in §222 of the Telecommunications Act of 1996, as amended, and the FCC’s regulations concerning CPNI. The Company’s policy is to ensure that all levels of personnel properly learn, implement and enforce rules and regulations concerning CPNI.

Pursuant to FCC regulations, the Company has implemented policies and procedures to ensure proper treatment of CPNI. All employees are required to learn and implement these procedures, or be subject to disciplinary action. This document constitutes the Company’s policies and procedures related to CPNI.

MCTI provides a primarily dispatch communications service with only ancillary interconnection with the public switched network. The service is classified by the FCC as Commercial Mobile Radio Service (“CMRS”) because of its ancillary interconnection feature. The Company does not claim co-carrier status with respect to its interconnection rights, but instead operates as a business user on the telephone network. All telephone numbers are in the Company’s name; the Company’s customers do not have individual telephone numbers associated with their two-way radios, but use an over dial capability to gain access to the telephone lines secured by the Company. Thus, the customer information to which the Company has access is not of the type that typically is considered CPNI or that might be expected to have value to any third party, thereby triggering the violations that the CPNI rules seek to prevent. Nonetheless, the Company recognizes that it is subject to the CPNI rules and has put in place the policies and procedures described herein to ensure its compliance with those requirements, including the policies and procedures that would be necessary should it provide telephone numbers to its customers in the future.

All employees are required to follow the policies and procedures described in this chapter.

II. Definition of CPNI

CPNI is information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier; except that such term does not include subscriber list information, which is subscriber names, addresses,

phone numbers and/or advertising classifications that a carrier or its affiliate have published, or provided for publication, in a telephone directory.

Such information includes account numbers, the Company's telephone numbers, bill amounts, call records, minutes used, plan information, features information, locations or numbers called, equipment, and other account information. Employees unsure of whether requested information contains CPNI should ask their supervisors for guidance.

III. Use of CPNI

MCTI does not provide or market categories *of service besides* CMRS. The Company may use, disclose, or permit access to CPNI without customer approval for the purpose of providing or marketing CMRS service offerings, including the marketing of handsets and data or Blackberry services.

MCTI does not use, disclose, or permit access to CPNI for marketing of any products not within the CMRS category of service or adjunct thereto. Should MCTI provide, market, or partner with another entity to market other categories of telecommunications service, these policies may be amended to reflect customer consent procedures consistent with state and federal law.

Prohibited Uses

The Company may not use, disclose, or permit access to CPNI to market non-commercial services, unless the customer has provided approval to do so (either opt-in or opt-out approval in accordance with FCC regulations). The Company may not use, disclose, or permit access to CPNI to track customer calls to competing service providers.

Permitted Uses

The Company may use CPNI to market CMRS services, or services that are adjunct to basic wireless services (information services), including, but not limited to, speed dialing, directory assistance, call waiting, call forwarding, caller I.D., text messaging, wireless data, and Blackberry services.

The Company may also use, disclose, or permit access to CPNI, without customer approval, for the following:

1. To provide customer premises equipment (CPE).
2. To provide wiring, installation, maintenance, and repair services;
3. To research health effects of wireless service;
4. To protect the rights of the Company or to protect other users or carriers from fraudulent, abusive, or unlawful use of such services;
5. To create, calculate, bill, and collect for service; and,
6. To provide call location information (E911) concerning the user in an emergency.

In response to a law enforcement agency in accordance with applicable legal requirements.

IV. Customer Authentication

The Company and its employees will take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI. All employees must properly authenticate a customer prior to disclosing CPNI during customer-initiated calls, online account access, or in-store visits.

Customer-Initiated Calls

“Call detail information” means any information pertaining to specific calls, including numbers called to/from, time, duration, or location of calls. *Amount of minutes used or remaining minutes of use are not call detail records.* When a customer calls a Company representative or authorized dealer, if any, the Company representatives may only disclose call detail information under the following circumstances:

1. If the customer gives his or her password, established online, if online customer care is used, or through the customer’s account. The password may not use readily available biographical information such as addresses, SSN, or driver’s license numbers. The representative may call the customer back at the wireless number associated with the requested records to establish a password for future call detail requests.
2. If the customer does not have a password, call detail information may be disclosed if the representative sends the information to the address on the customer account or by calling the customer back on the number associated with the requested records. Representatives may not call a different number to disclose information, and may not send the call detail records to any other address than that on the account.

If the customer is able to provide call detail information to the representative, then the representative may discuss the information provided by the customer.

In-Store and Dealer Inquiries

Retail sales associates and dealers, if any, may disclose CPNI to a customer, provided the customer presents a valid photo ID matching the customer’s account information.

Business Customers

The Company may utilize other authentication procedures not described here for services provided to businesses, provided that the account has a dedicated account representative, and that the account has a contract specifically addressing the Company’s protection of CPNI.

V. Notification of Account Changes

The Company will notify the customer via voicemail, text message, or US mail anytime a customer's password, response to back-up question, online account information, or address of record is created or changed. This notification is not required when the new customer initiates service, but is required when a current customer obtains a password online.

VI. Notification of CPNI Security Breaches

A "security breach" has occurred if a person has intentionally gained access to, used, or disclosed CPNI without authorization.

In the event of a security breach, the Company's management will notify the United States Secret Service and the Federal Bureau of Investigation. Law enforcement notification will occur within seven (7) days of discovery of the security breach. The Company will not disclose the breach to the customer or the public until seven (7) days after law enforcement notification.

Once law enforcement has been notified and seven (7) days have passed, the Company will notify its customer[s] of the CPNI security breach. The Company will also keep electronic or other records of any breaches discovered, of law enforcement notifications, and of customer notifications for at least two (2) years.

VII. Company safeguards and Recordkeeping

Management Safeguards

1. Training of Company personnel and dealers, if any, with access to CPNI will include review of the CPNI policies and procedures herein for all new employees and all existing employees who have not previously gone through the training process. Additional training will be provided as-needed.
2. The Company has designated a CPNI Compliance Officer who is responsible for: (1) communicating with the Company's attorneys and/or consultants regarding CPNI responsibilities, requirements and restrictions; (2) supervising the training of Company employees and agents who use or have access to CPNI; (3) supervising the use, disclosure, distribution or access to the Company's CPNI by independent contractors and joint venture partners, if any; (4) maintaining records regarding the use of CPNI in marketing campaigns, should that occur; and (5) receiving, reviewing and resolving questions or issues regarding use, disclosure, distribution or provision of access to CPNI.

Company personnel will make no decisions concerning CPNI without first consulting the Compliance Officer: Stephen Muensterman

3. In deciding whether the Company use of CPNI is proper, the Compliance Officer will consult these policies, FCC regulations, and legal counsel as necessary.
4. In accordance with FCC regulations, the Compliance Officer will ensure that the Company enters into confidentiality agreements with partners or contractors to whom it discloses CPNI (for which it has received customer approval), in the event such disclosures are contemplated.
5. Files containing CPNI are maintained in a secure manner such that they cannot be used, accessed, disclosed or distributed by unauthorized individuals or in an unauthorized manner.
6. The Company takes reasonable measures to discover and protect against activity that is indicative of pretexting, including requiring Company employees and agents to notify the CPNI Compliance Officer immediately to report any suspicious or unusual activities that might indicate pretexting efforts.
7. Any improper use of CPNI will result in disciplinary action in accordance with the Company's disciplinary policies. Violation of these policies and procedures will be treated as a serious offense, and may result in suspension or termination of employment.
8. On an annual basis, a Corporate Officer will sign a compliance certificate, to be filed with the FCC prior to March 1st, stating that he or she has personal knowledge that the Company has established operating procedures that are adequate to ensure compliance with the FCC's rules.

Recordkeeping

1. The Company will maintain records of any sales and/or marketing efforts that use CPNI, including a description of each campaign and the products or services offered.
2. The Company will maintain records of all instances in which it discloses CPNI to third parties, including each campaign or project, the purpose of the disclosure, and the information disclosed.

All records concerning CPNI, including court orders concerning CPNI, will be maintained for a minimum of one (1) year in a readily available and identifiable separate file.