



CROCKER & CROCKER, P.C.
ATTORNEYS AT LAW

PATRICK D. CROCKER
patrick@crockerlawfirm.com

February 25, 2009

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

Filed Electronically Via ECFS

RE: Total Call Mobile, Inc.
Customer Proprietary Network Information Certification
EB Docket No. 06-36

Dear Ms. Dortch:

Pursuant to 47 C.F.R. 64.2009(e) please find attached the 2008 Annual CPNI Certification and Accompanying Statement filed on behalf of Total Call Mobile, Inc.

Please contact the undersigned should you have any questions or concerns at (269) 381-8893 or patrick@crockerlawfirm.com.

Very truly yours,

CROCKER & CROCKER, P.C.


Patrick D. Crocker

PDC/tld

cc: FCC Enforcement Bureau (2 copies via USPS Mail)
Best Copy and Print, Inc. (via e-mail FCC@BCPIWEB.COM)

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

EB Docket 06-36

Annual 64.2009(e) CPNI Certification for 2008

Date filed: February 27, 2009

Name of Company Covered by this Certification: Total Call Mobile, Inc.

Form 499 Filer ID: Pending

Name of Signatory: Mark E. Leafstedt

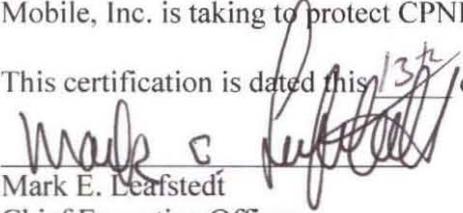
Title of Signatory: Chief Executive Officer

I am the Chief Executive Officer of Total Call Mobile, Inc. and as such do hereby certify, affirm, depose, and say that I have authority to make this Customer Proprietary Network Information ("CPNI") Annual Certification of Compliance on behalf of Total Call Mobile, Inc. I have personal knowledge that Total Call Mobile, Inc. has established adequate operating procedures to ensure compliance with the Commission's CPNI rules as set forth in 47 C.F.R. § 64.2001 et. seq.

Attached to this Certification is an Accompanying Statement explaining how the company's procedures ensure compliance with the requirements set forth in section 64.2001 et seq. of the Commission's rules.

Total Call Mobile, Inc. received no customer complaints in the past year concerning the unauthorized release of CPNI. Further, Total Call Mobile, Inc. has taken no action against data brokers for the unauthorized release of CPNI during calendar year 2008. Total Call Mobile, Inc. will report any information it may obtain with respect to the processes pretexters are using to attempt to access CPNI and what steps Total Call Mobile, Inc. is taking to protect CPNI.

This certification is dated this 13th day of February, 2009.


Mark E. Leafstedt
Chief Executive Officer
Total Call Mobile, Inc.

**ACCOMPANYING STATEMENT REGARDING TOTAL CALL MOBILE, INC.
CUSTOMER PROPRIETARY NETWORK INFORMATION (CPNI)
OPERATING PROCEDURES**

February 27, 2009

Total Call Mobile, Inc. ("TC Mobile" or "Company") provides this statement pursuant to 47 C.F.R. § 64.2009(e) to explain how TC 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.

Certification

TC Mobile requires an officer of the Company to sign and file with the Commission a compliance certification on an annual basis. The certification is based on the personal knowledge of the certifying officer, acquired through personal information and inquiry, that TC Mobile has established operating procedures designed to ensure compliance with the Commission's CPNI rules. TC Mobile's certifying officer relies in part upon information provided by corporate officers and managers directly responsible for implementing the Company's CPNI operating procedures.

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

TC Mobile does not 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 TC Mobile change its policies such that the use, disclosure, or permitted access to CPNI requires customer approval, appropriate customer notice, record-keeping, and FCC notification practices will be implemented.

Consistent with the Commission's rules, although TC Mobile does not necessarily engage in each of the following activities, TC 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 Services (CMRS)) to which the customer already subscribes without customer approval;
- provisioning customer premises information (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 to protect 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, TC Mobile does not 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, TC Mobile is not required to provide customer notice regarding CPNI rights as prescribed in the Commission's rules. Should TC Mobile change its policies such that customer notice is required, such notice will be provided.

Record Retention for Marketing Campaigns

TC Mobile maintains 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. TC Mobile maintains such records for at least one year.

Reporting Opt Out Failures

TC Mobile's policy is to not use, disclose, or permit access to its customers' CPNI without customer approval except as permitted under the Commission's rules or as otherwise provided in Section 222 of the Communications Act of 1934, as amended. Should TC Mobile change its policies and seek customer approval to use, disclose, or permit access to CPNI, TC 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

TC Mobile has a supervisory review process that governs its use of CPNI. As a general matter, employees must receive permission from their supervisors or other authorized personnel before using or disclosing CPNI for sales or marketing purposes.

Safeguarding CPNI

TC Mobile takes the privacy and security of CPNI seriously. In addition to its internal policies, which are designed to ensure compliance with the Commission's CPNI Rules, TC Mobile publishes online its Terms & Conditions of service, which explains how TC Mobile uses, discloses, and protects customer information, including CPNI, consistent with applicable law.

General Privacy and Security Measures

TC Mobile has implemented numerous controls to ensure compliance with the FCC's CPNI rules. For example, TC Mobile has in place a team of employees whose responsibilities focus on, among other things, CPNI protection and compliance. Additionally, CPNI released to TC Mobile's sales agents is specifically protected from disclosure through confidentiality provisions contained in TC Mobile's dealer agreement with its agents. TC Mobile agents must protect CPNI in their possession from unauthorized disclosure and must advise their employees, sub-agents, and similar individuals of their obligation to protect the CPNI. Additionally, the confidentiality provisions of the dealer agreement by their terms survive any termination of the dealer agreement. TC Mobile also undertakes other privacy precautions through its electronic data retention policy, such as removing historical billing information from its central customer database after a certain period of time.

Customer Authentication Procedures

TC Mobile has established procedures that require proper authentication prior to disclosing CPNI based on customer-initiated telephone contacts, in-store visits, and online. TC Mobile does not disclose call detail information over the telephone in response to customer-initiated telephone contacts unless the customer provides a previously-established Personal Identification Number or "PIN" that is not prompted by TC Mobile requesting readily available biographical or account information. If TC Mobile cannot authenticate a customer through the PIN process, TC Mobile either will randomly-generate and transmit a PIN via SMS text message to the telephone number of record and have the customer confirm the PIN once it is received before disclosing call detail information on a customer-initiated call, or TC Mobile will disclose call detail information only by calling the customer at the telephone number of record or by transmitting the information to the address of record. TC Mobile requires a valid government-issued photo ID matching the customer's account information prior to disclosing CPNI during a visit to a retail store. Online account access to CPNI is permitted only with a password – initially established through use of a randomly-generated Personal Identification Number or "PIN" delivered to the customer by means of an SMS text message to the telephone number of record. TC Mobile also provides optional account passwords outside the online environment (e.g., for calls to customer care); but if these passwords are established using customer biographical information, they are not used as an authentication method by TC Mobile for the release of call detail CPNI to end users.

Employee Training Program

TC Mobile provides Company-wide training to educate and train its personnel regarding the confidentiality of customer information, including authorized and unauthorized uses of CPNI. As part of their training, employees are provided with a document titled "CPNI 101," which explains CPNI and TC Mobile's policies regarding the proper use and safeguarding of CPNI. Employees must acknowledge that they have read the training document. In addition, all TC Mobile employees must affirmatively acknowledge, on an annual basis, that they have received and agree to abide by TC Mobile's Professional and Business Code of Conduct, which is incorporated as part of the employee handbook. The Code of Conduct explains that all customer information, including CPNI, must be maintained in the strictest of confidence and

may not be disclosed except as authorized and necessary when performing duties for TC Mobile.

Employee Discipline Program

TC Mobile has a 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 TC 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

TC Mobile mails a notice to the customer's address of record within 48 business hours whenever, among other changes, a password for access to call detail CPNI, customer response to a back-up means of authentication for such lost or forgotten passwords, online account, or address of record is created or changed. 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 address provided at account activation). Any such notice does not include or reveal the changed information.

Notice of Security Breaches

TC Mobile notifies 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.

TC Mobile strives 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 disclose or notify customers. TC Mobile respects any agency request that TC 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

A record of CPNI security breaches, notifications made to law enforcement, and notifications made to customers is maintained for at least two years.

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 in the prior year is included along with the annual certification to the Commission.

A record of any actions taken by TC Mobile against data brokers is maintained and an explanation of such actions included with the annual certification to the Commission, including any information TC Mobile has with respect to the processes pretexters are using to attempt to access CPNI.