



# CHINA UNICOM USA CORPORATION

Received & Inspected

MAR -2 2009  
FCC Mail Room

February 23, 2009

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

**Section 64.2009(e) Annual CPNI Certification**

**EB Docket No. 06-36**

China Unicom USA Corporation  
Form 499 Filer ID: 824402

I, Yitao Wu, V.P. of China Unicom USA Corporation ("China Unicom" or the "Company")), hereby certify that I am an officer of the Company and, acting as an agent of the Company, have personal knowledge that China Unicom has established operating procedures that are adequate to ensure compliance with the Federal Communications Commission's ("Commission") Customer Proprietary Network Information rules, 47 C.F.R. §§ 64.2001 *et seq.* (the "CPNI Rules"). Attached to this certification is an accompanying statement explaining how the Company's procedures ensure that it is in compliance with the CPNI Rules.

China Unicom did not take any actions (proceedings instituted or petitions filed at state commissions, the court system, or at the Commission) against data brokers in 2008. Furthermore, the Company did not receive any customer complaints concerning the unauthorized release of CPNI in 2008.

Yitao Wu  
Vice President

No. of Copies rec'd \_\_\_\_\_  
List ABCDE \_\_\_\_\_

*Internal Procedure of CPNI Compliance*  
CHINA UNICOM USA CORPORATION

CHINA UNICOM USA CORPORATION (“CUUSA” or the “Company”) received global Section 214 resale and facilities-based authority from the FCC in 2002. CUUSA is compliance with the FCC’s rules for protecting the privacy of customer proprietary network information (“CPNI”).

As FCC required, it is CUUSA’s duty to protect the confidentiality of proprietary information of, and relating to, other telecommunication carriers, equipment manufacturers, and customers, including telecommunication carriers reselling telecommunications services (including Internet access or voice mail services) provided by CUUSA.

According to FCC, CPNI is defined as:

- i). 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
- ii). Information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier,
- iii). Except that such term does not include subscriber list information.

Under the CPNI rules, the Company is not prohibited from using, disclosing, or permitting access to CPNI it obtains from its customers to (i) initiate, render, bill, and collect for telecommunications services; (ii) protect the rights or property of the Company, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services; (iii) provide any inbound telemarketing, referral, or administrative services to the customer for the duration of the call, if such call was initiated by the customer and the customer approves of the use of such information to provide such service; and (iv) provide call location information concerning the user of a commercial mobile service or the user of an IP-enabled voice service for purposes of assisting in the delivery of emergency services in response to an emergency in accordance with CPNI rules.

As part of the CPNI rules, the Company must properly authenticate a customer prior to disclosing CPNI based on customer-initiated telephone contact, online account access, or an in-store visit.

To safeguard CPNI, the Company requires its employees to follow the policies as below:

1. The Company currently prohibits the use of CPNI to market the Company’s services.

2. *Employees are not allowed to conduct any marketing without internal oversight and approval to ensure the CPNI requirements are followed.*
3. All Company employees will be provided with a copy of these procedures and receive training as to when they are and are not authorized to use CPNI.
4. In case of any violations of the Company's CPNI policies by any employee, CUUSA will take disciplinary action against him/her, up to and including termination.
5. CUUSA is not currently in need of sales and marketing campaigns. However, in the future, if such process is undertaken, the Company will establish a process to obtain any necessary "opt in" and "opt out" consents from customers and to maintain any applicable CPNI-related record. Such record includes all instances where CPNI was disclosed or provided to third parties, or where third parties were allowed access to CPNI. The record must 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. The record will be kept for a minimum of one year.
6. CUUSA does not provide customers with retail or online access to CPNI, but in the event of customer-initiated telephone contact with CUUSA, the Company must authenticate the identity of the caller in accordance with FCC rules before disclosing that customer's CPNI.
7. Mr. Yitao Wu, the V.P. of the Company, will serve as its CNPI Corporate Officer who is responsible for overseeing the Company's compliance with the CPNI requirements. The CPNI Corporate Officer will sign and file with the FCC a compliance certificate on an annual basis stating that he has personal knowledge that the Company has established operating procedures that are adequate to ensure compliance with the FCC's CPNI rules and provide a statement to accompany the certificate that explains how the Company's operating procedures ensure that it is, or is not, in compliance with the FCC's CPNI rules.
8. In case of any breach of CPNI, the Company will notify the FCC, law enforcement and customers about this breach at the earliest possible time in accordance with FCC rules.
9. The Company will track and maintain a summary of any actions taken against data brokers and a summary of all customer complaints received that concern the unauthorized release of CPNI.

Some exceptions will take place under the following circumstances:

- i) CUUSA may allow its authorized employees to use, disclose, or permit access to CPNI for the purpose of providing or marketing service offerings among the categories of service (i.e., local, inter-exchange, and CMRS) to which the customer already subscribes, without customer approval. Mr. Yitao Wu is in charge of this special authorization.
- ii) CUUSA may use, disclose, or permit access to CPNI, without customer approval,

*in its provision of inside wiring installation, maintenance, and repair services, or,*  
for the purpose of conducting research on the health effects of CMRS. Such actions  
must be approved by Mr. Yitao Wu in advance.

**STATEMENT OF CPNI COMPLIANCE:  
CHINA UNICOM USA CORPORATION**MAR - 2 2009  
FCC Mail Room

February 23, 2009

China Unicom USA Corporation ("China Unicom" or the "Company") has established internal operating procedures pursuant to Section 222 of the Communications Act of 1934, as amended (47 U.S.C. § 222) and Section 64.2001 *et seq.* of the rules of the Federal Communications Commission to safeguard the use and dissemination of customer proprietary network information ("CPNI").

China Unicom provides telecommunications services in, to or from the United States to established customers, but otherwise currently does not engage in marketing activities, and thus does not use CPNI for marketing purposes. It also does not provide CPNI to any affiliated or non-affiliated third parties, except as necessary to provide the services and as permitted in Section 222(d) of the Communications Act.

China Unicom safeguards CPNI by:

- Training employees regarding the Company's policy that prohibits the use of CPNI to market the Company's services;
- Instructing employees not to conduct any marketing without internal oversight and approval to ensure the CPNI requirements are followed (and to establish appropriate consumer consent mechanisms if they are required);
- Taking disciplinary action against employees for any violations of the Company's CPNI policies;
- Establishing a process to maintain any applicable CPNI-related records (including any sales and marketing campaigns that the Company may undertake in the future);
- Designating a corporate officer who is responsible for overseeing the Company's compliance with the CPNI requirements; and
- Establishing procedures for notifying the FCC, law enforcement and customers in the event of any breaches of CPNI.

In accordance with Section 64.2009(e) of the FCC's rules, to China Unicom's knowledge no CPNI was obtained by any data broker or unauthorized third party in 2007. China Unicom took no actions (proceedings instituted or petitions filed at state commissions, the court system, or at the Commission) against data brokers in 2007, and it received no customer complaints in 2007 regarding the unauthorized release of CPNI.