

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

**EB Docket 06-36**

Annual 64.2009(e) CPNI Certification for 2010 covering the prior calendar year, 2009.

Date filed: 2/26/2010

Name of company(ies) covered by this certification: **U.S. TelePacific Corp., Mpower Communications Corp. & Arrival Communications, Inc., all d/b/a TelePacific Communications**

Form 499 Filer IDs: 819502/817290/803442

Name of signatory: Russell Shipley

Title of signatory: Sr. V-P, Wholesale & Network Services

Certification:

I, Russell Shipley, 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 that are adequate to ensure compliance with the Commission's CPNI rules. *See 47 C.F.R. § 64.2001 et seq.*

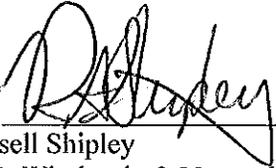
Attached to this certification is an accompanying statement explaining how the company's procedures ensure that the company is in compliance with the requirements (including those mandating the adoption of CPNI procedures, training, recordkeeping, and supervisory review) set forth in section 64.2001 *et seq.* of the Commission's rules. Statement attached.

The company has not taken actions (i.e. proceedings instituted or petitions filed by a company at either state commissions, the court system or the Commission against data brokers) against data brokers in the past year.

The company has received two customer complaints in the past year concerning the unauthorized disclosure of CPNI, which are summarized immediately below.

- The company received one report of unauthorized disclosure of CPNI; upon investigation, it was found that information had been provided regarding trouble with outgoing e-mail, which is a data service, not technically covered by CPNI. Nonetheless, the company is strengthening its procedures to protect all confidential customer information. See attached statement.
- As a result of an automated notice of changed password to an on-line account, the company also received a complaint regarding unauthorized access to online information; upon investigation, it appeared that the IP address had been spoofed; a new password was immediately instituted.

The company represents and warrants that the above certification is consistent with 47 C.F.R. Sec. 1.17 which requires truthful and accurate statements to the Commission. The company also acknowledges that false statements and misrepresentations to the Commission are punishable under Title 18 of the U.S. Code and may subject it to enforcement action.

By:   
\_\_\_\_\_  
Russell Shipley  
SVP, Wholesale & Network Services

Supporting Statement re CPNI Procedures --  
TelePacific Communications companies

- The TelePacific companies (“TelePacific” or “Company”) have mandated procedures for verifying that the Call Center, Repair and other customer-facing personnel are providing CPNI only to authorized customers and users.
  - TelePacific instituted strict procedures for matching callers with authorized user information in its databases and for calling out to main telephone numbers to contact authorized users, when needed.
  - TelePacific initially instituted manually-signed customer forms for authorization to use or change customer information, whether by internal customer representatives or on an on-going basis by agents of customers. TelePacific has subsequently modified these forms slightly for enhanced efficiency.
  - Forms initially were made available electronically and returnable, signed & on letterhead, by fax, e-mail, or mail. These are now back-up systems.
  - Company subsequently completed the development and implementation of automated e-mail confirmations of all changes to customer account information. More specifically, when talking to an authorized user who desires to update and/or change customer information, a pre-formatted e-mail can be completed & sent to an authorized user, with “voting buttons,” to return the e-mail with a confirmation, or denial, of change. These documents are automatically retained in company databases.
  - Company has actively sought updated or expanded information regarding authorized users, when in contact with an authorized user, and now “flags” accounts for which authorized user information has not been confirmed within the past six months.
  - Fraud control procedures provide for investigation of any automated e-mail confirmation which results in a denial of change.
- On-Line Systems: Password-related procedures for TelePacific on-line systems were upgraded to ensure they meet all aspects of the rules.
- When customer online databases are consolidated, customers are required to meet more restrictive password requirements and provide security questions.
- An authorized user is automatically notified of any account changes.
- Training: Extensive, required initial training sessions were held. Additional training sessions have been held on system upgrades such as the automated e-

mails. An explanation of basic CPNI requirements is provided on-line and in various documents, including the Employee Guidebook and the anti-fraud presentation made to all new sales personnel.

- Company is in the process of expanding and up-grading its training programs with the intent of assuring in depth and detailed new hire training for customer-facing personnel, as well as annual high-level reviews for all personnel, along with periodic CPNI awareness notices and campaigns.
- Breach Procedures: Breach prevention procedures were reviewed for completeness & effectiveness and company is in the process of establishing more detailed procedures for meeting any potential breach more quickly and efficiently.
- Company is also in the process of developing procedures which will allow for automated database retention and automated searches for reported breach-related information.
- Marketing: Company has long had required policies and procedures regarding use of CPNI for marketing, including supervisory review and record retention.
- Oversight & Review: In addition, to assure that all customer confidential information is protected, whether it is voice or data information, company has instituted an oversight and development committee to review procedures regarding processes related to protecting customer confidential information and to see that those processes are upgraded periodically as appropriate.