

**Annual 47 C.F.R. § 64.2009(e) CPNI Certification**  
**EB Docket 06-36**

Annual 64.2010(e) CPNI Certification for 2018

Date filed: 2/11/2019

Name of company covered by this certification: Royal Phone Company LLC

Form 499 Filer ID: 822532

Name of signatory: Tae Kim

Title of signatory: Executive Vice President

I, Tae Kim, 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.*

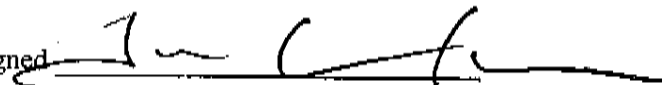
Attached to this certification is an accompanying statement explaining how the company's procedures ensure that the company is in compliance with the requirements set forth in section 64.2001 *et seq.* of the Commission's rules.

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

The company has not received any customer complaints in the past year concerning the unauthorized release of CPNI.

The company represents and warrants that the above certification is consistent with 47.C.F.R. § 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.

Signed



Attachments:

Accompanying Statement explaining CPNI procedures

Statement Regarding Operating Procedures Implementing 47 C.F.R. Part 64 Governing Use of Customer Proprietary Network Information

- I.
  - a. Royal Phone always authenticates a customer prior to disclosing CPNI based on customer-initiated telephone contact or online account access. Authentication is based on account information such as customer's address, customer's account number and/or amount of last bill. We do not store customer's social security number.
  - b. Royal Phone has only 1 employee in a single open office, and there is a very close supervision of employees to ensure that employees follow all procedures and to ensure that that CPNI is not disclosed in error.
  - c. Royal Phone is a single entity without subdivision so there is no passing of information between internal entities and we absolutely do not share CPNI information with external entities.
- II.
  - a. Account ID and Password is required for online access to CPNI by customers which the customer set up and only the customer can view. Royal Phone employees cannot see the password, but employees are able to reset passwords upon customer request.
  - b. Presently less than 150 customers access CPNI via online access to view their own phone bills.
- III. If a customer requests CPNI over the phone, it is sent only to the customer's address of record, or by calling the customer at the telephone number of record and only after the customer authenticates his/her identity and only after the supervisor approves the transmittal.
- IV. Except for use and disclosure of CPNI that is permitted without customer approval, or as otherwise described in section 64.2007(b) or otherwise provided in section 222, Royal Phone does not disclose, or permit access to its customer's CPNI by any external party or internal departments.
- V. All Royal Phone employees are trained to follow these guidelines to protect customer CPNI. Employees understand that any violation of these guidelines would result in

disciplinary action including suspension and/or dismissal from their position with the company. We have 1 employee who has been with the company for more than 12 years and we have not hired a new employee for the past 10 years.

- VI. Royal Phone has never been notified of any breach to customers CPNI since the establishment of the company and Royal Phone is currently not aware of any breach to customer CPNI. If breach is discovered, Royal Phone has a process in place to notify law enforcement (United States Secret Service and the Federal Bureau of Investigation) of the breach.