Accompanying Statement to Annual CPNI Compliance Certification for

IP Retail, Inc

In compliance with 47 C.F.R. 64.2009(e), I, Martin Toha, acting on behalf of IP Retail, Inc, certify the company has taken the following actions:

Restricted Use of CPNI and Notice To Customers:

- Our company has established reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI. Our company properly authenticates a customer prior to disclosing CPNI based on customer initiated telephone contact and online account access.
- Our company uses CPNI without customer approval to market enhancements to services customers' already use. If our company was to use CPNI for other marketing, we will obtain the customer's approval to do so. The company may request the customer's approval orally, in writing, or electronically. The request must contain specific disclosures about how our company will use the customer information. The content includes detailed information of data usage.
- Both opt in and opt out methods are used based on the particular usage of CPNI, as designated by 47 CFR 64.2007.
- The company provides 24/7 ability to opt out for all customers. The company's policy requires that they send out 'refresher" notices every 2 years.

Customer Authentication Methods:

- Instituted customer authentication methods to ensure adequate protection of customers' CPNI. We do not release call detail information based on customer initiated telephone contact. A customer can request call detail information to be sent to the customer's address of record. (Postal or electronic) that has been on the customer's account for 30 days. Customers requiring instant access to call detail information have the option of accessing such data online in the protected manner as stipulated.

Employee Training and Discipline:

- The company provides training and information about the usage of CPNI to all its employees, independent contractors, and other agents. They are trained in the proper usage of CPNI and there is an express disciplinary process for unauthorized use of CPNI. Violation by company employees, independent contractors, or agents of such CPNI requirements will lead to disciplinary action, depending upon the circumstances of the violation. Violation by Company independent contractors or joint venture partners of

such CPNI requirements will also lead to prompt disciplinary action (up to and including remedial training and termination of contract).

Marketing:

- All sales and marketing campaigns are subject to a three tier senior level approval process. We do not use individual records for marketing purposes.
- No outbound sales and marketing campaign can be conducted without management approval and any such campaign would require supervisory review to assure compliance with the CPNI rules
- Verified that the company enters into confidential agreements with all joint venture partners, independent contractors or any other third party when releasing CPNI.
- Guaranteed that the company only discloses CPNI to agents, affiliates, joint venture partners, independent contractors or to any other third parties only after receiving "opt in" approval from a customer.

Record Keeping Requirements

- Our company has established a system to maintain a record of all sales and marketing campaigns that use customers' CPNI, including marketing campaigns of affiliates and independent contractors.
- Ensured that these 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. Our company will make certain that these records are maintained for a minimum of one (1) year. The company keeps records of customer approval/rejection to use CPNI by storing the records in a secured database. (added punctuation)

Notification of CPNI Security Breaches

- Company employees, agents, independent contractors and joint venture partners are required to notify the CPNI Department of any access or security problems they encounter with respect to files containing CPNI.
- Our company shall notify law enforcement of a breach of its customers' CPNI.
- Our company will not notify its customers or disclose the breach publicly, whether voluntarily or under state or local law or these rules, until it has completed the process of notifying law enforcement.
- Our company will notify law enforcement, as soon as possible, and in no event later than seven (7) business days, after reasonable determination of the breach, we shall electronically notify the USSS and the FBI through the designated central reporting facility.

- We will not notify customers or disclose the breach to the public until seven 7 days have passed after notification to the USSS and the FBI except as provided in Section 64.2011.
- We maintain an electronic record of any breaches discovered, notifications made to the USSS and the FBI pursuant to paragraph (b), and notifications made to customers. The record must include, if available, dates of discovery and notification, a detailed description of the CPNI that was the subject of the breach, and the circumstances of the breach. The record shall be retained for a minimum of 2 years.