**Attachment:** Statement of CPNI Operating Procedures

**FUSION TELECOMMUNICATIONS INTERNATIONAL, INC.**

**STATEMENT OF CPNI OPERATING PROCEDURES**

1. It is the policy of Fusion Telecommunications International, Inc. (the “Company”) not to use, disclose, or permit access to Customer Proprietary Network Information (“CPNI”), as defined in the FCC’s rules, for any purpose other than the following, all of which are permitted without customer approval under FCC rules:

1. For the purpose of providing or marketing Company service offerings within categories of service (i.e. local, interexchange) to which the customer already subscribes.
2. For the purpose of providing inside wiring installation, maintenance, and repair services.
3. For the purpose of marketing “adjunct to basic” services, such as 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.
4. For the purpose of protecting the rights or property of the Company, or to protect use of its services and other carriers from fraud, abusive, or unlawful use of or subscription to such services.

2. The Company has established a program to inform and train personnel that they may not use, disclose, or permit access to CPNI for any purpose other than those set forth above. At present, the Company does not engage in outbound telemarketing using CPNI. The Company has an express disciplinary process in place to discipline violations of its CPNI policy.

3. Because the Company does not use, disclose, or permit access to CPNI, except as described above, by definition, it does not need to maintain a record of sales and marketing campaigns that use customers’ CPNI, or of instances where CPNI is disclosed to third parties, or where third parties were allowed access to CPNI.

4. Because the Company does not use CPNI, except as described above, the Company does not utilize a notification and customer approval process (i.e., an opt-out or opt-in process). If the Company changes its marketing procedures, an appropriate customer notification process will be instituted.

5. The Company’s online access system only provides access to basic account profile information. It does not provide access to call detail information. The Company does not provide online access to even this basic information until the customer has established a login ID and password that is consistent with the Company’s security policies and that does not rely on the use of readily available biographical information or account information.

6. Customers who contact the Company via inbound calls are not provided with call detail information. If a customer requests specific call detail information, the request is referred by the CSR to a supervisor. The supervisor will either (a) provide the requested information via a letter mailed to the customer contact at the customer’s address of record, or (b) via a return telephone call to the customer contact at the customer’s telephone number of record.

7. Customers who present themselves at the Company’s offices and who request CPNI are asked for proper photographic identification (e.g. a state-issued driver’s license, a passport, or equivalent identification). CPNI will be disclosed only if the customer presents valid photographic identification that matches the customer’s account information.

8. The Company has not detected any unauthorized access to CPNI, either by employees, pretexters, or other third parties during 2017.

9. The Company did not receive any customer complaints regarding CPNI during 2017, and did not take any actions against data brokers during 2017.

10. The Company will notify the customer immediately, if the customer’s address of record is created (except at the time of service initiation) or changed. This notification is made by mail to the customer’s pre-existing address of record, and does not reveal the changed information.

11. In the event of any breach of a customer’s CPNI, as described in Section 64.2011 of the FCC rules, the Company will, as soon as practicable and in all events within seven (7) days of determination of the breach, notify law enforcement through http://www.fcc.gov/eb/cpni, and subsequently notify the customers in accordance with the procedures and in the sequence prescribed in that rule section. The Company will maintain a record of any such breaches and notifications for at least two (2) years.

12. The Company has in place a supervisory review process regarding compliance with its CPNI policy.