**Blu Shield**
Shield Through Intelligence

## CPNI Compliance Statement and Operating Procedures

## of Code Blu Shield, LLC.

Pursuant to 47 U.S.C. § 222, and the relevant FCC CPNI Rules and Orders, Michael E. Payne Jr, Chief Information Officer, of Code Blu Shield, LLC D/B/A "Blu Shield" (hereinafter "Blu Shield" or "Company"), and affiliated entities makes the following statement:

Blu Shield provides data processing software and services to companies that sell telecommunications services, including retail wireless dealers, wireless carriers, business to business wireless dealers, and others ("Dealers"). Blu Shield's contracts contain confidentiality agreements that address the use and protection of customers' private information.

Blu Shield has established policies and procedures to comply with the Federal Communications Commission's ("FCC") rules regarding the use, disclosure, and access to section 62.2001 et seq. of the FCC's rules, 47 C.F.R. § 64.2001 et seq. These procedures ensure that the Company is compliant with the FCC's Customer Proprietary Network Information (CPNI) Rules and Orders.

Consistent with the rules of CPNI, the Company may use, disclose, and permit access to CPNI without customer approval (1) to render, bill, and collect for services provided; (2) to protect the rights or property of the Company, other users or other carriers from unlawful use; (3) for the purpose of software maintenance, repair, and troubleshooting; and (4) to comply with a valid legal process such as a subpoena, court order, or search warrant.

Blu Shield does not use, disclose, or permit access to CPNI for marketing purposes. The Company is therefore not required to seek approval from existing customers to use their CPNI and does not maintain a record of a customer's approval to use CPNI. Should Blu Shield change its marketing practices such that opt-out notices are required, the Company will implement procedures to ensure that customers are notified of the new practices and the customer's approval can be established prior to use of CPNI. Furthermore, the Company does not share, sell, lease or otherwise provide CPNI to any of its affiliates, suppliers, vendors, and any other third parties for the purposes of marketing any services.

The Company has implemented processes and procedures to train its personnel as to when they are and are not permitted to use CPNI and has completed such training and will periodically refresh such training (at minimum, annually). Blu Shield's CPNI Policy also provides guidance of how Company employees are required to use, maintain, and disclose CPNI. Those individuals who have access to customer's CPNI have specific performance requirements related to use and protection of CPNI and are subject to supervisory review. Any and all access to CPNI, by Company employees, automated system processes, or by authorized employees of Dealers and Carriers is logged and is subject to supervisory review by both the Company and the Dealer, or the Company and Carrier. Any employee found to have violated CPNI policy will be subject to disciplinary action up to and including termination.

**Blu Shield**
Shield Through Intelligence

Blu Shield has implemented measures for the recording and auditing of the access and use of CPNI by employees of the Company, and employees, partners, independent contractors, or any other third parties of the Dealer or Carrier. Such measures include:

a. All CPNI is stored in a separate database per Dealer. Each database is only accessible to the Company and the Dealer for which the database is provided.
b. Access to the database is limited by 1) secure login from the Blu Shield website using SSL and strict password requirements, 2) direct login by members of the Information Technology and Support departments of Blu Shield only. All logins are logged and subject to audit.
c. All logins via the website are recorded along with the end user's IP Address and geographical location (via GPS or by interpretation of IP Address).
d. Access to the website must be granted by an authorized representative of the Dealer, and must be created by an employee of Blu Shield or by an authorized representative of the Dealer. Website access can be terminated by Blu Shield at any time pursuant to an agreement with the Dealer and also by request of the authorized representative of the Dealer.
e. User web sessions are automatically terminated, requiring the user to login again, after an idle period.
f. All access to CPNI is recorded during a user's session on the website. The logs of user activity are subject to audit by both the Dealer and the Company.

Blu Shield has practices and procedures governing the disclosure of CPNI:

a. Blu Shield does not disclose or release CPNI upon a customer's telephone request.
b. Blu Shield does not disclose or release CPNI to customers through online access over the Internet.
c. Blu Shield does not have any retail locations where customers can obtain CPNI.

Blu Shield is prepared to notify the required U.S. government agencies in the event of a breach of the CPNI rules and to provide the required notice to affected customers of any such breach in accordance with the FCC CPNI Rules; that is, no later than seven days following the breach, to the United States Secret Service (USSS) and the Federal Bureau of Investigation (FBI) specified in 47 C.F. R. § 64.2011. Blu Shield's internal procedure is to notify the customer following notice to law enforcement unless there is an urgent need to notify the customer to prevent harm or law enforcement directs the Company to withhold any public disclosure for up to 30 days. Blu Shield retains electronic or manual records of all CPNI breaches for a minimum of two years.