



27 February 2008

Broadweave Networks
10813 South River Front Parkway
Suite 500
South Jordan, UT 84095

Certificate of Compliance

I, Steve Christensen, CEO of Broadweave Networks, personally certify that Broadweave Networks has the appropriate policies and procedures in place adequate to protect customer proprietary network information in accordance with the rules and regulations established by Section 222 of the Communications Act of 1934, as amended by the Telecommunications Act of 1996 and C.F.R Sec 64.2003 – 2009

Signed,

A handwritten signature in black ink, appearing to read "Steve Christensen", written over a horizontal line.

Steve Christensen
CEO

27 February 2008

Broadweave Networks
10813 South River Front Parkway
Suite 500
South Jordan, UT 84095

CPNI Compliance Procedures

Broadweave Networks' has a strict privacy policy in places which restricts the sharing and use of customer information—including, but not limited to CPNI.

Broadweave does not share CPNI with third parties. Internal use of CPNI is governed by Broadweave's policy document, **Broadweave CPNI Compliance Policy**. This document establishes procedures governing access, use, reporting, documentation and misuse of Broadweave's CPNI.

Signed,



Steve Christensen

27 February 2008

Broadweave Networks
10813 South River Front Parkway
Suite 500
South Jordan, UT 84095

Summary of Complaints Regarding Unauthorized Access to Customer CPNI

Broadweave has received no complaints regarding unauthorized access to customer CPNI.

Signed,



Steve Christensen

Accompanying Statement of Annual CPNI Compliance Certification

Indicate below (X) whether the Company has taken any or all of the following actions to protect against the unlawful disclosure of CPNI.

Employee Training and Discipline

- Trained all employees and personnel as to when they are and are not authorized to use CPNI.
- Instituted an express disciplinary process for unauthorized use of CPNI.

Sales and Marketing Campaign Approval

- Guaranteed that all sales and marketing campaigns are approved by management.

Record-Keeping Requirements

- Established a system to maintain a record of all sales and marketing campaigns that use their 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.
- Made certain that these records are maintained for a minimum of one (1) year.

Establishment of a Supervisory Review Process

- Established a supervisory review process for all outbound marketing situations.
- Certified that under this review process, all sales personnel obtain supervisory approval of any proposed outbound marketing request for customer approval.

Opt-in

- Guaranteed that the Company only disclosed CPNI to agents, affiliates, joint venture partners, independent contractors or to any other third parties only after receiving "opt-in" approval from a
- Verified that the Company enters into confidential agreements with joint venture partners, independent contractors or any other third party when releasing CPNI.

Opt-Out Mechanism Failure

- Established a protocol through which the Company will provide the FCC with written notice within five (5) business days of any instance where opt-out mechanisms do not work properly, to such a

Compliance Certificates

- Executed a statement, signed by an officer, certifying that he or she has personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the
- Executed a statement detailing how operating procedures ensure compliance with CPNI regulations.



Executed a summary of all customer complaints received in the past year concerning unauthorized release of CPNI.

Customer Authentication Methods



Instituted customer authentication methods to ensure adequate protection of customers' CPNI. These protections only allow CPNI disclosure in accordance with the following methods:



Disclosure of CPNI information in response to a customer providing a pre-established password;



Disclose of requested CPNI to the customer's address or phone number of record; and



Access to CPNI if a customer presents a valid photo ID at the carrier's retail location.

Customer Notification of CPNI Changes



Established a system under which a customer is notified of any change to CPNI. This system, at minimum, notifies a customer of CPNI access in the following circumstances:

--password modification;

--a response to a carrier-designed back-up means of authentication;

--online account changes; or

--address of record change or creation.

Notification of Law Enforcement and Customers of Unauthorized Access



Established a protocol under which the appropriate Law Enforcement Agency ("LEA") is notified of any unauthorized access to a customer's CPNI.



Ensured that all records of any discovered CPNI breaches are kept for a minimum of two (2) years.