CPNI Compliance Checklist

This checklist is designed to assist regulated telecommunications service providers address general compliance with the Federal Communications Commission's rules regarding the protection of Customer Proprietary Network Information, or CPNI. Companies with specific questions about CPNI compliance should contact The *Comm*pliance Group.

CPNI Security Measures

1. The company notifies customers of changes to CPNI stored in customer accounts.
2. Customers are provided password-protected logins for online access to CPNI.
3. Employees are prohibited from releasing CPNI over the telephone, except in one of these three (3) circumstances:
    a. The customer provides a pre-established password when calling the company;
    b. CPNI is sent to the customer's billing address; or,
    c. A company representative calls the customer's telephone number.
4. All user-generated passwords are based on non-biographical information.
5. Company employs a Personal Identification Number (PIN) system in addition to, or in place of, a user-generated password.
6. The company encrypts and/or password protects access to internal records and/or databases which contain CPNI.

Employee Training Policies

7. The company has instituted a program to oversee or supervise those employees with access to CPNI.
8. The company has enacted disciplinary procedures, such as reprimand, suspension, or termination proceedings, for employees who breach internal CPNI safeguards.

Use of CPNI in Marketing Campaigns

9. CPNI provided to a third party for marketing or advertising purposes is kept confidential.
10. The company maintains a record for one (1) year of all sales and marketing campaigns that use the CPNI. This record includes 1) a description of each campaign, 2) the specific CPNI that was used in the campaign, and 3) what products and services were offered as part of the campaign.
11. The company notifies customers individually of their right to restrict the use of, disclosure of, and access to CPNI prior to use in marketing campaigns (i.e., "opt-out" notification).
12. The company obtains opt-in approval for any instance when CPNI is used by a third party in marketing campaigns. (Note, opt-in approval is not required to share CPNI with a third party for non-marketing purposes).
13. Records of customer approval are maintained for at least one (1) year.

Third Party use of CPNI

14. The company mandates that third parties with access to CPNI maintain confidentiality.

Unauthorized Access to CPNI

15. The company has established internal procedures to alert the FCC to a failure of CPNI safeguards.
16. The company has established internal procedures to alert federal law enforcement agencies, specifically the United States Secret Service ("USSS") and the Federal Bureau of Investigation ("FBI"), to a failure of CPNI safeguards.
17. Records of any discovered CPNI breaches kept for a period of two (2) years.