

**CPNI Company Certification & CPNI Policy Statement**

**EB Docket No. 06-36**

**Gateway Telecom, LLC, d/b/a StratusWave Communications, LLC  
("StratusWave"); Filer ID No. 821764**

I, John Reasbeck, am chief financial officer of StratusWave. Pursuant to 47 U.S.C. § 222 of the Communications Act and 47 C.F.R. §64.2009, I hereby state that I am responsible for company compliance with the FCC's CPNI rules and have personal knowledge that StratusWave has established procedures that are adequate to ensure compliance with the rules. I further certify that StratusWave did not take any actions against data brokers in 2009, and that StratusWave received no customer complaints during 2009 regarding the unauthorized release of CPNI.

StratusWave's compliance is demonstrated in the attached CPNI Policy Statement.

  
\_\_\_\_\_  
John Reasbeck

February 26, 2010

## CPNI Policy Statement

1. Our company utilizes an employee training program with a disciplinary process and supervisory review to ensure compliance with CPNI rules and regulations.
2. All of the company's proprietary data bases, including that containing customer information, are password protected, and access to same is limited to authorized personnel only. Distribution of the password is limited to those authorized personnel. The password will be changed routinely, and whenever an employee with access to such data bases leaves the company.
3. No customer information in any form is to be removed from the company's offices by employees or others. This includes computer printouts, handwritten information or notes, copies of files or documents in any electronic form, and verbal transmission of customer information to persons who are not direct employees of the company.
4. Employees are to closely guard customer lists, contact information, telephone numbers, and all other customer information, both proprietary and public, to prevent any information from being removed from our offices by non-employees either accidentally or intentionally.
5. Disconnected or inactive customer files are to be retained for no more than 3 years, and then shredded. Disconnected or inactive customer files are never to be placed in the trash unshredded. Customer database printouts are to be shredded when replaced by newer printouts.
6. Our company has a supervisory approval process in place for any proposed outbound marketing request for CPNI.
7. Our company has a notification process in place to alert law enforcement, the FCC and affected customers in the event of a CPNI breach.
8. Our company requires a photographic identification from any customers requesting account information in our retail stores. Our company does not have a mechanism whereby customers can access their accounts online, so no password protection for online accounts is required. Our company requires that all requests for CPNI that come in by telephone be reduced to writing and sent to the Company via e-mail or paper, so no CPNI is released to customers on the telephone. Responses to customer inquiries are sent to the customer's address of record or previously-supplied e-mail account. Our company intends to implement a system for password protection of customer accounts that would enable online access, but has not yet done so.
9. Among other things, any online access system will include a notification process to provide immediate notice to customers when a customer-initiated password or backup for forgotten passwords, an online account, or the address of record, is created or changed.

10. Our company has a formal process in place to certify the CPNI protection policies instituted by our applicable vendors, service bureaus and wholesale carriers. Our company does not conduct joint marketing with these entities and therefore is not required to obtain opt-in consent from customers for joint marketing purposes.

11. Appropriate disciplinary action will be taken for any violations of this policy.