Annual 47 C.F.R. § 64.2009(e) CPNI Certification Template

EB Docket 06-36

Annual 64.2009(e) CPNI Certification for 2019 covering the prior calendar year 2018

1. Date filed: February 11, 2019
2. Name of company(s) covered by this certification: Stanton Telecom, Inc.
3. Form 499 Filer ID: 801165
4. Name of signatory: Robert J. Paden
5. Title of signatory: Vice President/General Manager
6. Certification:

I, Robert J. Paden, certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. *See* 47 C.F.R. § 64.2001 *et seq.*

Attached to this certification is an accompanying statement explaining how the company's procedures ensure that the company is in compliance with the requirements (including those mandating the adoption of CPNI procedures, training, safeguards, recordkeeping, and supervisory review) set forth in section 64.2001 *et seq.* of the Commission's rules.

The company has not taken actions (*i.e.,* proceedings instituted or petitions filed by a company at either state commissions, the court system, or at the Commission against data brokers) against data brokers in the past year.

The company has not received customer complaints in the past year concerning the unauthorized release of CPNI.

The company represents and warrants that the above certification is consistent with 47. C.F.R. § 1.17 which requires truthful and accurate statements to the Commission. The company also acknowledges that false statements and misrepresentations to the Commission are punishable under Title 18 of the U.S. Code and may subject it to enforcement action.

Signed Robert J. Paden

Attachments: Accompanying Statement explaining CPNI procedures

STATEMENT

Stanton Telecom, Inc. (the "Company") has established operating procedures that ensure compliance with the Federal Communications Commission regulations regarding the protection of customer proprietary network information ("CPNI"). These procedures include but are not limited to:

- The Company has appointed a CPNI Compliance Officer. The Compliance Officer is responsible for ensuring that the Company is in compliance with all of the CPNI rules and is the point of contact for anyone with questions about CPNI.
- The Company has established authentication procedures for providing both call detail and non-call detail information on a customer initiated call. If the customer comes into the office, the customer must provide a valid photo ID matching the customer's account information.
- The Company has a process to track and notify customers whenever a change is made to the customer's account. For example, a change of address is sent to the customer's old address of record to verify the address change.
- The Company has a process for reporting breaches that comply with the reporting requirements. A record of any breach will be maintained for a minimum of two years.
- The Company has not provided notification to its customers and has not asked for approval to use CPNI because it only uses CPNI in those instances where it is permissible to use CPNI without customer approval. The Company does not share CPNI with any joint venture partner, independent contractor or any other third party. For marketing purposes, the Company does not use CPNI because it does mass marketing to all customers. If in the future, the Company decides to ask customers for approval to use their CPNI, it will implement a system by which the status of a customer's CPNI approval can be clearly established prior to the use of any CPNI.
- The Company continually educates and trains their employees regarding the appropriate use of CPNI. The training includes, but is not limited to, when employees are and are not authorized to use CPNI. Employees are instructed that if they ever have any questions regarding the use of CPNI, if they are aware of CPNI being used improperly by anyone, or if they encounter someone other than the authorized person on an account trying to access CPNI that they should contact the Compliance Officer immediately.
- The Company has established specific disciplinary procedures should an employee violate the CPNI procedures established by the Company. The disciplinary procedures are reviewed with employees and are kept in a permanent Company file.
- The Company does not conduct any marketing campaigns that use customer's CPNI at this time, but it does have a supervisory review and approval process documented that must be followed if the Company's sales personnel make a decision to conduct a marketing campaign. The Company will ensure that a record of any marketing campaign of its own, or its affiliates, will be maintained for a minimum of one year. The record will include a description of the campaign, the specific CPNI that was used in the campaign and what products and services were offered as part of the campaign.
- The Compliance Officer will ensure that a compliance certification signed by an officer of the company is filed with the FCC by March 1 of each year. A copy of the certification will be kept permanently.
- The Company's CPNI procedures include reasonable measurers to discover and protect against activity that is indicative of pretexting or any other type of unauthorized access to CPNI. Employees are instructed to notify the Compliance Officer immediately of any suspicious activity.