Smithville COMMUNICATIONS

1600 West Temperance Street • Ellettsville, IN 47429
(800) 742-4084 • smithville.com

February 21, 2018

FILED ELECTRONICALLY

Marlene H. Dortch

Office of the Secretary
Federal Communications Commission
445 12th Street, SW
Suite TW-A325
Washington, DE 20554

Re: EB Docket No. 06-36

Dear Ms. Dortch:

On behalf of Smithville Communications, Inc., Form 499 Filer ID 805743 pursuant to §64.2009 (e) of the Commission's rules, I am attaching the CPNI Compliance Certificate and the Accompanying Statement as required.

Please contact me with any questions at 812-935-2215.

Regards,

Stephanie Wall

Stephanie Wall
Regulatory Compliance Accountant

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

EB Docket 06-36

Annual 64.2009(e) CPNI Certification for 2018 covering the prior calendar year 2017.

1. Date filed: February 21, 2018
2. Name of Company covered by this Certification: Smithville Communications Inc.
3. Form 499 Filer ID: 804117
4. Name of signatory: Darby A. McCarty
5. Title of signatory: CEO
6. Certification:

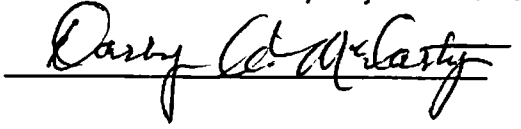
I, Darby A. McCarty, certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. *See* 47 C.F.R. Section 64.2001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

Attachments: Accompanying Statement explaining CPNI procedures

Smithville Communications, Inc.
Customer Proprietary Network Information (CPNI) Policy
(47 CFR 64.2001-64.2011)

When referred to in the guidelines set forth below, "Company", "we", or "us" refers to and includes all employees, associates and agents of Smithville Communications.

Smithville Communications (the Company) has a duty to protect the confidential Customer Proprietary Network Information (CPNI) of our customers, other telecommunications carriers and equipment manufacturers.

CPNI is any information that relates to the quantity, technical configurations, type, destination and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship. CPNI also includes information contained in the bills pertaining to the telephone exchange service or telephone toll service received by a customer of a carrier.

Proprietary information of our customers, other telecommunications carriers and equipment manufacturers, is protected by Federal law.

CPNI which the company obtains from another carrier for the purpose of providing a particular telecommunications service may be used only for the provision of that service, and may not be used for any otherwise unrelated marketing efforts.

Individually identifiable CPNI that we obtain by providing a telecommunications service may be used, disclosed, or released only in the circumstances as set forth later in this CPNI Policy.

The release of any CPNI by sales personnel must be authorized by a supervisor.

The Company takes seriously the protection of our customers' CPNI and in accordance with 47 CFR 64.20009(e) (amended) will be subject to disciplinary review for violation of the policies set forth above. Therefore, the following guidelines shall be followed by all employees and agents of the Company:

<u>Customer Notification Policy</u>

The Company will annually notify and inform each customer of his or her right to restrict the use or disclosure of, and access to, CPNI along with a solicitation of opt-out approval.

The Company will maintain records of that notification, whether oral or written, for at least one year.

The notification will provide information sufficient to enable our customers to make informed decisions as to whether to permit the use or disclosure of, or access to, their CPNI.

The notice will contain a statement that the customer has a right, and we have a duty under federal law, to protect the confidentiality of their CPNI.

The notice will specify the types of information that constitute CPNI and the specific entities that will receive CPNI, describe the purposes for which the CPNI will be used, and inform the Customer of his or her right to disapprove those uses and deny or withdraw access to CPNI use at any time. With regard to the latter, we indicate that any approval or disapproval will remain in effect until the Customer affirmatively revokes or limits such approval or denial.

The Company will advise the customer of the precise steps the customer must take in order to grant or deny access to CPNI and clearly state that a denial of approval will not affect the provision of any services to which the customer subscribes.

The statement will be in a clear and neutral language, which describes the consequences directly resulting from the lack of access to CPNI. In addition, we may state that the customer's consent to use his or her CPNI may enhance our ability to offer products and services tailored to meet the customer's needs and that we will disclose the customer's CPNI to any person upon the affirmative written request of the customer.

The notice will not include any statement that attempts to encourage a customer to freeze third-party access to CPNI.

New customers will be verbally notified at the time of the request for service.

Use of CPNI

The Company will use, disclose or permit access to CPNI to protect our rights, property, customers and other carriers from fraudulent, abusive or unlawful use of, or subscription to, our services.

The Company will use, disclose or permit access to CPNI to provide or market service offerings among the different categories of service – local, interexchange, etc., to which the customer already subscribes from the Company.

When the Company provides different categories of service, and a customer subscribes to more than one service category, we share the customer's CPNI with the affiliate that provides service to the customer; but if a customer subscribes to only one service category, we do not share the customer's CPNI with an affiliate without the customer's approval.

We use, disclose or permit access to CPNI derived from our provision of local exchange or interexchange service for the provision of CPE and call answering, voice mail or messaging, voice storage and retrieval services, and protocol conversion without customer approval.

Without customer approval, we do not use, disclose or permit access to CPNI to provide or market service offerings within a category of service to which the customer does not already subscribe, except that we use, disclose or permit access to CPNI to do the following: a) provide inside wiring installation, maintenance and repair services; b) services such as, but not limited to, speed dialing, computer-provided directory assistance, call monitoring, call tracing, call blocking, call return, repeat dialing, call tracking, call waiting, caller ID, call forwarding and certain Centrex features.

The Company will not use, disclose or permit access to CPNI to identify or track customers that call competing service providers. For example, as a local exchange carrier we do not use local service CPNI to track customers that call local service competitors.

Should our company provide CMRS or VoIP services, we will comply with Part 64.2005 (c) (3) as the rules relate to these services.

Approval or Disapproval of CPNI

We honor a customer's approval or disapproval until the customer revokes or limits such approval or disapproval.

Subject to "opt-out" approval requirements, we use a customer's individually identifiable CPNI to market communications-related services to that customer and we disclose that CPNI to our affiliates that provide communications-related services. We also allow these to obtain access to such CPNI to market communications-related services.

Under the Commission's "Notice Requirements Specific to Opt-Out" provisions, we will wait a minimum of 30 days after giving customers notice and an opportunity to opt-out before assuming customer approval to use, disclose, or permit access to CPNI.

In addition, under the Opt-Out mechanism we will notify customers every two years, and other Opt-Out provisions per Part 64.2008(d) will be followed.

Since we disclose and allow access to customers' individually identifiable CPNI to our affiliates, we require, in order to safeguard that information, confidentiality agreements that:

a. Require our affiliates' use of the CPNI only for the purpose of marketing or providing the communications- related services for which CPNI has been provided.

b. Disallow their permitting any other party to use, allow access to, or disclose the CPNI to any other party, unless they are required to make disclosure under force of law.
c. Require that they have in place appropriate protections to ensure the ongoing confidentiality of the CPNI.

Customer Authentication for Call Detail

Since the release of call detail information over the telephone presents an immediate risk to privacy, the Company is prohibited from releasing call detail information based on customer-initiated telephone contact, except under these four circumstances:

a. When a customer provides a pre-established password.
b. When a customer requests that the information is sent to the customer's address of record.
c. When a representative of our company calls the telephone number of record and discloses the information.
d. At retail locations, we may continue to provide account access to customers who present valid photo ID's.

If a customer initiates a call, password protection is not required for routine customer care procedures regarding service/billing disputes or questions if the customer is able to provide all of the call detail information necessary to address the customer question (i.e. telephone number called, when it was called, amount charged for the call).

The Company will provide mandatory password protection for online account access. Online access based solely on a customer's readily available biographical information is prohibited. However, the Company is not required to reinitialize existing passwords for online customer accounts.

Establishing a Password

For existing customers, the Company must first authenticate the customer by either calling the account number on record or the customer presenting a valid photo ID in person at any retail location.

For a new customer, the Company may establish a password at the time of service initiation and the customer may be authenticated at that time.

Customer Account Authentication

We will authenticate the customer for their protection and confirm the person we are speaking with is the account holder. Authentication may include, but is not limited to, the following:

a. City of birth
b. Childhood pet
c. Other names listed on the account

We will not discuss the following account information with a spouse, child, parent, etc. unless they are authorized by the account holder. Account information may include, but is not limited to, the following:

a. Name
b. Address
c. Phone Number
d. SSN
e. Billings or charges
f. Balance due or payment status

A maximum of four authorized contacts may be added to the account by the authorized account holder.

All documents, notes, and printed materials with customer information will be shredded and disposed of properly. This may include, but is not limited to, the following:

a. Social Security Number
b. Customer's name, address and phone number
c. Copy of bill or remittance slip

Law Enforcement

All requests originating from a law enforcement agency for customer account or billing information will be directed to the Human Resources manager or another member of the Human Resources Department.

Notice of Account Changes

The Company must notify a customer immediately of account activity, such as a change to a password, on-line account, or address of record. Notification may be sent by email, voice mail, text message, or US Mail to the customer's address of record.

Notice of Unauthorized Disclosure or Breach of CPNI

If there has been a breach of CPNI, the Company must provide electronic notification of the breach within seven business days to the United States Secret Service (USSS) and the Federal Bureau of Investigation (FBI). The FCC provides a link for the reporting of

breaches at www.fcc.gov/eb/CPNI/. In order to allow law enforcement time to conduct an investigation, the Company must wait another seven business days before notifying the affected customers of the breach (unless the USSS and/or FBI request that the carrier continue to postpone disclosure). However, the Company may notify customers sooner if there is a risk of immediate and irreparable harm. In addition, we must keep records of discovered breaches for at least two years.

Joint Venture and Independent Contractor Use of CPNI

The Company must obtain opt-in consent from a customer before disclosing a customer's CPNI to a joint venture partner or an independent contractor for the marketing of communications-related services to the customer.

Business Customers

The Company may establish contract authentication procedures for business customers that are different from residential customers, so long as those customers have a dedicated account representative and the contracts specifically address the protection of CPNI.

CPNI Compliance Policy Statement

The Company has implemented a system by which the status of a customer's CPNI approval can be clearly established prior to the use of the CPNI.

We have trained our personnel as to when they are and are not authorized to use CPNI.

Any unauthorized use, sale, or otherwise disclosure of CPNI by any employee would subject the employee to disciplinary action. For the first violation, an employee will be given a warning and the violation will be noted on the employee's record. An employee will be subject to termination of employment for a second violation.

The Company maintains a record of our own and our affiliates' sales and marketing campaigns that use Customer's CPNI. The record includes a description of each campaign, the specific CPNI that was used in the campaign, and what products and services were offered as part of the campaign. We retain these records for at least one year.

Notification records and approval or disapproval records will be retained for at least one year.

The Company has established a supervisory review process regarding compliance with the CPNI rules for outbound marketing situations and we maintain compliance records for at least one year. Specifically, our sales personnel obtain supervisory approval of any proposed outbound marketing request for customer approval of the use of CPNI.

The Company has a corporate officer who acts as agent for the Company and signs a compliance certification on an annual basis before March 1 of each year in EB Docket No 06-36 stating that the officer has personal knowledge that the Company has established operating procedures adequate to ensure compliance with applicable CPNI rules. We provide a statement accompanying the certificate that explains our operating procedures and demonstrates compliance with the CPNI rules. In addition, we will include an explanation of any actions taken against data brokers and a summary of all customer complaints received in the past year concerning the unauthorized release of CPNI.