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

EB Docket 06-36

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

Date filed: February 28, 2019

Name of company covered by this certification**:** Mid-Rivers Telephone Cooperative Inc.

Form 499 Filer ID: 804663

Name of signatory: Dennis Green

Title of signatory: President

I, Dennis Green, 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 any 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 any 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.

Dennis Green, President

Attachment: Accompanying Statement explaining CPNI procedures

STATEMENT

The operating procedures of Mid-Rivers Telephone Cooperative, Inc., are designed to ensure compliance with the CPNI rules applicable to their operations. These procedures are outlined below.

I. CPNI Use

(1) We use, disclose or permit access to CPNI to protect our rights and property, and to protect our Customers and other carriers from fraudulent, abusive or unlawful use of, or subscription to, our services.

(2) We use, disclose or permit access to CPNI to provide or market service offerings among the categories of service (such as local, interexchange, Internet, video services or wireless) to which the Customer already subscribes. When we provide 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 do not disclose CPNI to joint venture partners or independent contractors.

(3) We use, disclose or permit access to CPNI derived from our provision of local exchange, exchange access or interexchange service for the provision of Customer Premises Equipment (CPE) and call answering, voice mail or messaging, voice storage and retrieval services, fax store-and-forward, and protocol conversion, without Customer approval.

(4) Without Customer approval, we will 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: (a) provide inside wiring installation maintenance and repair services; and (b) market services formerly known as adjunct-to-basic 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.

(5) We do 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. We do not use, disclose or permit access to a former customer's CPNI to regain their business when they have switched to a competing service provider.

(6) We will use, disclose or permit access to CPNI in conformance with the Customer's approval.

II. CPNI Use: Procedures for Access to and Customer Approval

(a) **Inbound Customer Contact** – In the context of an inbound Customer telephone contact requiring or requesting access to or use of the Customer's CPNI for the duration of the call, we (1) authenticate the identity of the Customer requesting access to CPNI information, as provided in Section II(e), and otherwise follow procedures provided in Sections II(f) and (g) below; (2) if a Customer requests "call detail" (information pertaining to the transmission of specific telephone calls, including the number called or from which the call was placed, the time, location or duration of any call), we require the Customer to provide an established password, as provided in Section II(f); and (3) request oral approval from the Customer during the course of the inbound telephone call in which the Customer's CPNI will be used. We understand we bear the burden of demonstrating that such approval was given in compliance with the CPNI rules**.** Upon receipt of oral approval, we use the Customer's individually identifiable CPNI to market communications-related services to that Customer during the call.

(b) **CPNI Notice Procedures for Inbound Calls**

(i) For each inbound call for which we seek Customer approval to use CPNI to market during the call, we inform the Customer of his or her right to restrict the use of CPNI, disclosure of, and access to the Customer's CPNI.

(ii) During the call and prior to seeking the customer's consent to use CPNI, we provide information sufficient to enable the Customer to make an informed decision as to whether to permit the use or disclosure of, or permit access to the CPNI. We: (a) advise that the Customer has a right, and we have a duty, under federal law, to protect the confidentiality of CPNI; (b) specify the types of information that constitute CPNI and the specific entities that will receive CPNI; (c) describe the purposes for which the CPNI will be used; and (d) 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 either the Customer affirmatively revokes or limits such approval (or disapproval) or the end of the telephone call, whichever first occurs.

(iii) We advise the Customer of the steps the Customer must take in order to grant or deny access to CPNI, and we clearly state that a denial of approval will not affect the provision of any services to which the Customer subscribes. However, we may provide a brief statement, in clear and neutral language, that 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. We inform the Customer that we will disclose the

Customer's CPNI to any person upon the affirmative written request of the Customer.

(iv) Our oral advisory during the telephone call is comprehensible and not misleading.

(v) We do not include in the advisory any statement that attempts to encourage a Customer to freeze third-party access to CPNI.

(c) **Procedures for Online CPNI Access** – In the context of customer online access to CPNI, we (1) authenticate the identity of the Customer requesting access to CPNI information, as provided in section II(e) below; and (2) require the Customer to provide an established password, as provided in Section II(f)below.

(d) **Procedures for In-Store CPNI Access** – In the context of customer access to CPNI at Company's retail locations, the Customer is required to present to the Company's agent a valid government-issued photo identification matching the Customer's account information.

(e) **Authentication Procedures** – A customer will be authenticated without use of readily available biographical information (information drawn from the customer's life history, including such things as the customer's social security number or any portion thereof, the customer's mother's maiden name, the customer's home address, or date of birth) or account information (including such items as account number or any component thereof, the telephone number associated with the account, or the bill's amount). The Company will, from time to time, establish authentication procedures (for example, assign randomly-generated Personal Identification Numbers ("PINs"), back-up customer authentication methods in the event of a lost or forgotten password (again, without prompting the customer for biographical or account information), such as PINs or shared secrets.

(f) **Password Protection Procedures** – New customers must establish a password at the time of service initiation. To establish a password, the Company will first authenticate the customer, as provided above. Passwords are not prompted by the Company's asking for readily available biographical information (information drawn form the customer's life history, including such things as the customer's social security number or any portion thereof, the customer's mother's maiden name, the customer's home address, or date of birth) or account information (including such items as account number or any component thereof, the telephone number associated with the account, or the bill's amount). Back-up authentication methods, as described above, may be established by the Company from time to time, but if a Customer cannot provide the correct password or the correct response for the back-up customer authentication method, the Customer will be required to establish a new

password, as provided herein. Repeated unsuccessful attempts to log in online will result in blocked access.

(g) **Alternative Access to Call Detail** – If a customer does not provide a password during a customer-initiated telephone request for call detail or correctly answer the shared secrets, the Company will not disclose such information during the call, but may offer to disclose call detail information by sending it to the customer's address of record (a postal or electronic address that the Company has associated with the Customer's account for at least 30 days), or by initiating a call to the Customer at its telephone number of record (the number associated with the underlying service, as opposed to any other telephone number the Customer may have supplied as an additional contact point). If the Customer is able to provide call detail information to the Company during a customer-initiated call without the Company's assistance, the Company will discuss the call detail information provided by the Customer.

III. CPNI Use Approval: Procedure for Opt-Out Approval

(a) In addition to the notice procedures described in Section II(b) above, when seeking "opt-out"[1] approval for the use, disclosure or access to CPNI, we use the following procedures:

(i) After providing written or electronic notice, an opportunity to "opt-out" or refuse permission to use, disclose or access CPNI (such notice being clearly legible, in sufficiently large type and conspicuously placed on the notice so as to be readily apparent to a Customer), we wait a minimum of thirty (30) days before assuming that the Customer has approved use, disclosure or access to CPNI. The written or electronic notice includes a clear statement identifying the specific time period we will wait before assuming that the Customer approves of our use, disclosure or access to the Customer's CPNI. We inform the Customer that in the case of an electronic notification, the waiting period begins and runs from the date the notification is sent; and in the case of notification by mail, the waiting period begins and runs from the third day following the date that the notification was mailed.

(A) Electronic mail notices are sent to Customers ONLY after our receipt of express, verifiable prior approval for e-mail notifications regarding a Customer's service in general, or CPNI in particular.

[1] The term "opt-out approval" refers to a method for obtaining customer consent to use, disclose, or permit access to the customer's CPNI. Under this approval method, a customer is deemed to have consented to the use, disclosure, or access to the customer's CPNI if the customer has failed to object thereto within the waiting period described in §64.2008(d)(1) after the customer is provided appropriate notification of the carrier's request for consent consistent with the rules in this subpart. [§64.2003(l)]

(B) We allow Customers to reply directly to e-mails containing CPNI notices in order to opt-out of approval for the use, disclosure or access to CPNI.

(C) If an e-mail opt-out notice is returned as undeliverable, we will send the Customer notice in another form before we consider the Customer to have received notice.

(D) When we utilize e-mail to send CPNI notices, we ensure that the subject line of the message clearly and accurately identifies the subject matter of the e-mail.

(ii) Opt-out notices are provided at a minimum every two (2) years.

(iii) Customers will be able to opt-out in a manner that (a) causes no additional cost to the Customer; and (b) is available 24 hours per day, seven days a week.

IV. CPNI Use Approval: Recordkeeping and Effectiveness

We maintain all records of Customer approvals for at least two (2) years.

Approvals and disapprovals to use, disclose or permit access to CPNI remain in effect until the customer affirmatively revokes or limits such approval or disapproval.

V. CPNI Safeguards

(1) We have implemented a system by which the status of a Customer's CPNI approval can be clearly established prior to the use of the CPNI. Oral approval of Customer consent to use CPNI for the duration of an in-bound call is maintained with the record of the call. Opt-out approval is determined and recorded at one staff level, then verified before customer service representatives or marketing personnel will have access to such information. Opt-out notations are readily and immediately apparent when a Customer's record is accessed for any purpose.

(2) We have trained our personnel as to when they are, and are not, authorized to use CPNI. In addition to a detailed description of Company expectations contained in the Company handbook (the details of which are available to the FCC upon request and subject to appropriate protective arrangements in light of its proprietary nature),

new hires for customer representative positions receive one-on-one training specifically with respect to their CPNI obligations, and the Company requires such personnel to acknowledge their responsibilities. Customer service representatives and department heads regularly receive ongoing CPNI training and education, including attendance at focused seminars and weekly meetings during which CPNI issues are raised and discussed.

(3) We have an express disciplinary process in place to deal with employee failures. Employees are aware of the seriousness of any infraction related to CPNI and that such infractions are placed upon the most severe disciplinary tract.

(4) Supervisors regularly monitor interaction with Customers to ensure that the Company's policies and directives are executed.

(5) Access to Customer records is restricted internally to personnel who require such access to perform their jobs.

(6) The Company aggressively monitors the database, and the hardware components are designed to record unauthorized access attempts. Such attempts are pursued immediately and rigorously.

(7) We maintain a record of our own and our affiliates' sales and marketing campaigns that use Customers' CPNI. We also maintain records of all instances wherein CPNI was disclosed or provided to third parties, or where third parties were allowed access to 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 two (2) years.

(8) We have established a supervisory review process regarding our compliance with the FCC's CPNI rules for outbound marketing, and maintain records related to compliance with those processes for a minimum of two (2) years. Sales personnel must obtain supervisory approval of any proposed outbound marketing request using Customers' CPNI.

(9) We have a corporate officer who acts as agent for the Company, that oversees the Company's compliance with the FCC's CPNI rules. This officer is charged with the duty to sign and file with the FCC a compliance certificate on an annual basis. This certificate states that the officer has personal knowledge that the Company has established operating procedures that are adequate to ensure compliance with CPNI rules. We provide a Statement accompanying the Certificate that explains how our operating procedures ensure that the Company is in compliance with the FCC's CPNI rules. Also included in the annual certificate is an explanation of any actions taken against data brokers, and a summary of all customer complaints received in the preceding year concerning the unauthorized release of CPNI. This filing is made annually on or before March 1 for data pertaining to the previous calendar year.

(10) In the event that our opt-out mechanisms do not work properly, to such a degree that a consumer's inability to opt-out is more than an anomaly, we will provide written notice within five (5) business days to the Federal Communications Commission, in the form of a letter identifying the Company and including a description of the opt-out mechanism(s) used, the problem(s) experienced, the remedy proposed and its implementation date, whether the relevant state commission was notified and if the state commission took any action, a copy of the notice provided to customers, and Company contact information.

(11) We have established a program designed to discover and protect against attempts to gain unauthorized access to CPNI, which includes authentication of the Customer's identity prior to disclosing CPNI during a customer-initiated telephone contact, online account access, or an in-store visit.

(12) We notify Customers immediately whenever a change has been made to an account or service, including a password, customer response to a back-up means of authentication for lost or forgotten passwords, online account, or when the address of record is changed (except when the customer initiates service, including the selection of a password at service initiation). This notification may be given through the U.S. Postal Service, a voice-mail or text message by the Company to the telephone number of record; such message will not reveal the changed information or be sent to the new account information.

(13) For business customers, the Company may establish different authentication regimes than those described herein for services provided to business customers that have a dedicated account representative that specifically addresses the Company's protection of CPNI.

(14) Notification of Security Breaches: The Company shall notify electronically the United States Secret Service and the Federal Bureau of Investigation of a breach in its customers' CPNI as soon as practicable, and in no event later than seven (7) business days, after reasonable determination of the breach. Only after the passage of seven (7) full business days after such notice to law enforcement as described in the preceding sentence will the Company notify customers or publicly disclose such breach, provided that if the carrier believes that there is an extraordinarily urgent need to notify any class of affected customers sooner than provided above in order to avoid immediate and irreparable harm, it shall so indicate in its notice to law enforcement and proceed to notify such affected customers only after consultation with the relevant investigating agency. Such notification shall not occur if the relevant investigating agency determines that public disclosure or notice to customers would impede or compromise an ongoing or potential criminal investigation or national security, for such initial or extended period as determined to be reasonably necessary in the judgment of the agency, and such determination is

provided in writing. After complying with the foregoing process of notifying law enforcement as provided herein, the Company shall notify its Customers of the breach of those Customers' CPNI. Records of notifications made to law enforcement and customers shall be kept, and shall include dates of discovery and notifications of the breach, a detailed description of the CPNI that was the subject of the breach, and the circumstances of the breach. Such records shall be retained for a minimum of two (2) years.