FALL RIVER RURAL ELECTRIC COOPERATIVE

Where Service Matters

FALL RIVER RURAL ELECTRIC COOPERATIVE, INC.

GENERAL POLICY NO 502
SUBJECT: MEMBER DATA PRIVACY POLICY

I. POLICY:

It shall be the policy of the Cooperative to take all reasonable steps to identify, detect, and prevent the theft of its members' personal information.

II. PURPOSE:

The Cooperative hereby adopts the following policy for: (1) identifying and detecting Red Flags; (2) responding to Red Flags; (3) preventing and mitigating Identity Theft; and (4) use of meter communication data. This is required under the federal regulations at 16 C.F.R. § 681.2 *et seq.*

III. DEFINITIONS

The term "identifying information" means any name or number that may be used alone or in conjunction with any other information, to identify a specific person, including name, social security number, date of birth, official state or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number, or address including E-mail address if available.

The term "Identity Theft" means a fraud committed or attempted using the identifying information of another person without authority.

The term "Red Flag" means a pattern, practice, or specific activity that indicates the possible existence of Identity Theft.

The terms "member" or "members" for purposes of this policy include both members of the Cooperative and non-member patrons of the Cooperative.

The term Advanced Metering Infrastructure "AMI" means a meter device

sometimes referred to as a smart meter which is measuring power usage; will allow two-way communication capability for the member as well as the Cooperative to collect and use data. A member will be able to monitor power usage of that meter, allowing them to make informed decisions.

IV. IDENTIFICATION OF ACCOUNTS SUBJECT TO RED FLAG POLICY

The Cooperative maintains accounts for its members that allow the members to pay for service after it has been rendered. Power usage is tracked from the member's service AMI and transmitted to the Cooperative allowing for two-way communication of commands for monitoring by the member if desired. Bills are sent and payments are due on a monthly basis. The Cooperative does not offer banking or financial services. The only other form of credit offered by the Cooperative to its members is the option to pay for line extension costs over time as a part of the member's monthly bill. The Cooperative also maintains as a part of its member accounts (1) utility deposits, when required for new service under its tariff; and (2) a Patronage Capital account for which retirement checks may be issued to members on a periodic basis. These accounts are all covered by this Red Flag policy.

V. IDENTIFICATION OF POTENTIAL RED FLAGS

A. Risk Factors. In identifying potential Red Flags associated with the accounts that the Cooperative maintains, the Cooperative's Board of Directors and management have considered the following Identity Theft risk factors:

1. **Types of Covered Accounts.** The Cooperative is an Electric Cooperative serving portions of rural Idaho, Montana, and Wyoming, providing its members with electric utility service. Member accounts can consist of four different components:

   a. **Payments for Utility Services Rendered.** Payments from members for services rendered are due by the due date listed on the billing statement. The Cooperative does not regularly provide credit to its members beyond this revolving, monthly

account for utility service. Such service is rendered at a fixed physical location known to the Cooperative, as a result, there is a low risk of misuse of identifying information to perpetrate fraud on the Cooperative for utility services rendered. However, identifying information maintained by the Cooperative could be used to perpetrate Identity Theft and defraud other businesses if the information was wrongfully altered or disclosed.

b. **Payments for Line Extensions.** For some line extensions, members may have the option of paying off the costs of the extension over time through their electric bills. Line extensions are constructed at a fixed physical location known to the Cooperative. As a result, there is a low risk of misuse of identifying information to perpetrate fraud on the Cooperative for line extensions that are paid for over time. However, identifying information maintained by the Cooperative could be used to perpetrate Identity Theft and defraud other businesses if the information was wrongfully altered or disclosed.

c. **Utility Deposits.** For some new members, utility deposits are required prior to the initiation of service. These amounts are held under the terms and conditions of utility's tariff and may eventually be refunded to the member. There is some risk that a member who is a victim of Identity Theft could have the member's utility deposit refunded to an identity thief. Additionally, identifying information maintained by the Cooperative could be used to perpetrate Identity Theft and defraud other businesses if the information was wrongfully altered or disclosed.

d. **Patronage Capital Accounts.** All members are eligible for allocation of patronage capital in accordance with the Cooperative's Bylaws and Board policies. Patronage capital is retired in accordance with the Bylaws and Board

policies, either in the form of a check to the member or a credit on the member's bill. There is some risk that a member who is a victim of Identity Theft could have the member's patronage capital retirement check sent to an identity thief. Additionally, identifying information maintained by the Cooperative could be used to perpetrate Identity Theft and defraud other businesses if the information was wrongfully altered or disclosed.

2. **Methods for Opening Accounts**. The Cooperative requires that prospective members who wish to receive utility service submit a membership application with the following information: (1) name of adult household members on the account; (2) address location where service shall be provided; (3) contact and billing information; and (4) Social Security Number or Tax Identification Number, or a copy of a valid Government issued photo identification may also be accepted if the member chooses not to provide their Social Security Number. 5) Business License or Articles of Incorporation. If the prospective member is physically in the office, the applicant must also present to the Member Service Representative, a valid Government-issued photo identification as proof of identity.

3. **Methods for Accessing Accounts**. The Cooperative allows members to access information related to their accounts using the following methods:

   a. In person at Fall River Rural Electric Cooperative, Inc's offices with a picture identification or other identifying information

   b. Over the telephone after providing the Cooperative's Member Service Representative with certain identifying information, such as the caller's name, the member's name, address and telephone number of the service location and the member's Social Security Number or Tax Identification Number, or additional information needed to verify identity.

c. By logging into the Cooperative's website, using a personal password or sign in on a member's account.

4. **Previous Experience with Identity Theft**. The Cooperative is not aware of any security breach of, or unauthorized access to, its systems that are used to store members' identifying information.

5. Information transmitted from a member's smart meter or commands or tasks sent from the Cooperative to the meter will be used by the Cooperative to more effectively serve the member and will not endanger private and personal information by sharing such with any other person or business without express consent and permission by those listed on the member's account.

B. **Sources of Red Flags.** In identifying potential Red Flags associated with the accounts that the Cooperative maintains, the Cooperative's Board of Directors and management have considered the following sources of Red Flags for Identity Theft:

1. **Past Incidents of Identity Theft**. As described in Section V.A.4 above, the Cooperative is not aware of any security breach of, or unauthorized access to, its systems that are used to store members' personal identifying information collected by the Cooperative. In the event of incidents of Identity Theft in the future, such incidents shall be used to identify additional Red Flags and this policy will be amended accordingly.

2. **Identified Changes in Identity Theft Risk**. As provided in Section VIII below, The Cooperative will at least annually review this policy, the utility's operations, and the utility's experience with Identity Theft for changes in Identity Theft risk.

3. **Applicable Supervisory Guidance**. In addition to considering the guidelines initially published with the FTC's Red Flag regulations, as a part of its annual review, the Cooperative will review additional regulatory guidance from the FTC and other consumer protection

authorities. This review shall focus on new Identity Theft risks and recommended practices for identifying, detecting, and preventing Identity Theft.

C. **Categories of Red Flags.** In identifying potential Red Flags associated with the accounts that the Cooperative maintains, the Cooperative's Board of Directors and Management have considered the following categories of Red Flags for Identity Theft, and will take the following actions upon discovering such Red Flags:

1. **Alerts, Notifications, and Warnings**. Alerts, notifications, or other warnings received from consumer reporting agencies or service providers, such as fraud detection services can be Red Flags for Identity Theft. Such alerts, notifications, and warnings include:

   a. A fraud or active duty alert is included in a consumer report.

   b. A consumer reporting agency provides a notice of credit freeze in response to a request for a consumer report.

   c. A consumer reporting agency provides a notice of address discrepancy.

   d. A consumer report indicates a pattern of activity that is inconsistent with the history and usual pattern of activity of an applicant or member, such as:

      1) A recent and significant increase in the volume of inquiries;

      2) An unusual number of recently established credit relationships;

      3) A material change in the use of credit, especially with respect to recently established credit relationships; or

      4) An account that was closed for cause or identified for abuse of account privileges.

The Cooperative does not generally apply for or receive consumer reports related

to its members. For this reason, the Cooperative does not anticipate receiving any consumer reports that might alert it to potential Identity Theft related to a member. However, if the Cooperative does receive such a report, Member Service Representatives shall report such activity to supervisors for further review and inquiry.

2. **Suspicious Documents**. The presentation of suspicious documents can be a Red Flag for Identity Theft. Presentation of suspicious documents includes:

   a. Documents provided for identification that appear to have been altered or forged.

   a. The photograph or physical description on the identification is not consistent with the appearance of the applicant or member presenting the identification.

   b. Other information on the identification is not consistent with information provided by the person opening a new account or member presenting the identification.

   c. Other information on the identification is not consistent with readily accessible information that is on file with the Cooperative, such as a membership application card.

   d. An application appears to have been altered, forged, or gives the appearance of having been destroyed and reassembled.

Member Service Representatives and other personnel of the Cooperative shall report to management when it appears that account documents have been altered or forged when compared to other documents in a member's file. It shall also be brought to a supervisor's attention immediately if any member presents an invalid identification, or identification that appears forged for the purpose of obtaining access to account information.

3. **Suspicious Personal Identifying Information**. The presentation of suspicious personal identifying information, such as a suspicious address change, can be a Red Flag for Identity Theft. Presentation of suspicious personal identifying information occurs when:

   a. Personal identifying information provided is inconsistent when compared against external information sources used by the Cooperative For example:

      1) The address does not match any address in the consumer report; or

      2) The Social Security Number has not been issued or is listed on the Social Security Administration's Death Master File.

   b. Personal identifying information provided by the member is not consistent with other personal identifying information provided by the member. For example, there is a lack of correlation between the Social Security Number range and date of birth.

   c. Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the Cooperative, for example:

      1) The address on an application is the same as the address provided on a fraudulent application; or

      2) The phone number on an application is the same as the number provided on a fraudulent application.

d. Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the Cooperative. For example:

   1) The address on an application is fictitious, a mail drop, or a prison; or

   2) The phone number is invalid or is associated with a pager or answering service.

e. The Social Security Number provided is the same as that submitted by other persons opening an account or other members.

f. The address or telephone number provided is the same as or similar to the account number or telephone number submitted by an unusually large number of other persons opening accounts or other members.

g. The person opening the covered account, or the member fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete.

h. Personal identifying information provided is not consistent with personal identifying information that is on file with the Cooperative

i. The person opening the account, or the member cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.

The Cooperative shall provide members access to their account information in person at the utility's offices only after verifying the member's identity through photo identification. Access to member account information via telephone or internet shall require the member to verify their identity using information that

would only be known to the member as reflected in the member's account. Member Service Representatives shall be trained to make note in a member's file when there is a lack of correlation between information provided by a member and information contained in a file for the purposes of gaining access to account information. Fall River Rural Electric Cooperative, Inc. is not to provide account information without first clearing any discrepancies in the information provided.

4. **Suspicious Activity**. The unusual use of, or other suspicious activity related to, a member account is also a Red Flag for potential Identity Theft. Suspicious activities include:

   a. Shortly following the notice of a change of address for a member account, the Cooperative receives a request for the addition of authorized users on the account.

   b. Mail sent to the member is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the member's covered account.

   c. The Cooperative is notified that the member is not receiving paper account statements.

   d. The Cooperative is notified of unauthorized charges or transactions in connection with the member's account.

   e. A member requests a patronage capital check or utility deposit refund check be sent to a new address without requesting a service disconnection or change in service location.

   f. A member requests that a patronage capital check or utility deposit refund check be made payable to a person other than the member.

   g. A member requests that the Cooperative provide the member with personal identifying information from the Cooperative's records.

Member Service Representatives shall be trained to note unusual use of accounts, or suspicious activities related to accounts and verify the identity of members in such circumstances. It shall further be the policy of the Cooperative to not provide identifying information to members, either verbally or in writing, even when members are asking for their own information. Member Service Representatives shall immediately notify management, who will conduct further reasonable inquiry, when a member requests such information. It shall be the policy of the Cooperative to train its Member Service Representatives to look for unusual activity when reviewing member accounts for service. Member Service Representatives shall also notify a supervisor when there are an unusually high number of inquiries on an account, coupled with a lack of correlation in the information provided by the member. For requests for Cooperative membership lists for use in Cooperative elections, the Cooperative shall take steps to ensure that the requested information is only disclosed in accordance with its General Policy #506 Member Access to Cooperative Information & Use of Membership Lists.

5. **Notices**. Notices of potential Identity Theft are also serious Red Flags, including:

   a. Notice from members, law enforcement authorities, or other persons indicating that a member has been a victim of Identity Theft;

   b. Notice to the Cooperative that a member has provided information to someone fraudulently claiming to represent the Cooperative;

   c. Notice to the Cooperative that a fraudulent website that appears similar to the Cooperative's website is being used to solicit members' personal identifying information;

   d. The Cooperative's mail servers are receiving returned e-mails that the Cooperative did not send, indicating that its members

may have received fraudulent e-mail soliciting members' personal identifying information.

Upon notice from a member, law enforcement authority, or other persons that one of its members may be a victim of Identity Theft, the Cooperative shall contact the member directly in order to determine what steps may be necessary to protect any member information in the possession of the Cooperative. Such steps may include, but not be limited to, setting up a new account for the member with additional identifying information that may be identified only by the member in order to protect the integrity of the member's account, or notifying members and the media of an on-going attempt to perpetrate a fraud on the membership.

VI. DETECTING RED FLAGS

A. It shall be the policy of the Cooperative to obtain identifying information about, and verify the identity of, a person opening an account. The Cooperative will obtain the member's name, date of birth, address for service location, and Social Security Number or Tax Identification Number to open a new account. The Cooperative may also require presentation of valid government-issued identification to open a new account. It shall be the policy of the Cooperative to not provide identifying information to members, either verbally or in writing, even when a member is asking for their own information.

B. It shall be the policy of the Cooperative to authenticate members and customers, monitor transactions, and verify the validity of change of address requests, in the case of existing accounts.

VII. PREVENTING AND MITIGATING IDENTIFY THEFT

A. If the Cooperative discovers that any of its members have become victims of Identity Theft; the Cooperative shall take appropriate steps to mitigate the impacts of such Identity Theft. These steps may include, but are not limited to:

1. Monitoring an account for evidence of Identity Theft;

2. Contacting the member;

3. Changing any passwords, security codes, or other security devices that permit access to an account;

4. Reopening an account with a new account number;

5. Closing an existing account;

6. Not attempting to collect on an account;

7. Notifying the member;

8. Notifying law enforcement; or

9. Putting a stop payment on any outstanding patronage capital refund or utility deposit refund checks;

10. Putting a hold on any new patronage capital refund or utility deposit refund checks;

11. Determining that no response is warranted under the particular circumstances.

B. The Cooperative has a business relationship with a third-party contractor taking customer payments or collections on past due accounts. Under this business relationship, the third-party contractor has access to member identifying information covered under this Policy. The CEO/General Manager shall ensure that the third-party contractor's work for the utility is consistent with this policy by (a) amending the contract to incorporate these requirements; or (b) by determining that the third-party contractor has reasonable alternative safeguards that provide the same or a greater level of protection for member information as provided by the Cooperative.

VIII. POLICY UPDATES AND ADMINISTRATION

A. The Cooperative shall consider updates at least annually to determine whether it has experienced any Identity Theft of its members' accounts, whether changes in the methods of Identity Theft require updates to this

policy, and whether changes are necessary to detect, prevent, and mitigate Identity Theft. The Cooperative's management will continue to monitor changes in methods of Identity Theft and re-evaluate this policy in light of those changes. A review of such changes should occur on an annual basis.

B. Administration of this Policy shall be as follows:

1. The Board of Directors has adopted this policy and will have ultimate authority over this policy, but the policy shall be managed by the CEO/General Manager of the Cooperative. The CEO/General Manager shall have authority to delegate oversight and compliance to other individuals at the senior management level. The CEO/General Manager shall be responsible for reviewing staff and management reports regarding compliance with the utility's policy.

2. Potential changes to the policy should be reviewed at least annually by Cooperative management. Material changes to the policy that may be needed prior to the meeting described herein shall be brought to the CEO/General Manager's attention and reviewed by management and the Board of Directors if deemed necessary by the CEO/General Manager.

3. Reports.

   a. Management personnel assigned responsibility under this policy or by delegation from the CEO/General Manager shall prepare a report, at least annually, regarding the implementation and progress of the utility's policy for review by the CEO/General Manager. The CEO/General Manager may, at their discretion, bring any issues related to the policy to the attention of the Board of Directors for review.

   b. The above-described report prepared by management personnel designated with supervising the policy shall include a discussion

of: the progress of implementing and the effectiveness of the policy; ongoing risk level of Identity Theft of member information; potential changes to the policy and other operation practices of the utility to further the goal of protecting member's personal information; and, identification and discussion of instances of Identity Theft of the utility's members.

c. The CEO/General Manager shall keep records of meetings regarding this policy showing the dates and topics discussed. The CEO/General Manager shall also cause a file to be maintained with copies of the five (5) most recent annual reports prepared under the policy.

IX. PRIMACY OF POLICY:

This policy supersedes any existing policy, which may be in conflict with the provisions of this policy.

APPROVED BY THE CEO/GENERAL MANAGER

Bryan L Case

Bryan Case, CEO/GM

DATE APPROVED: October 27, 2008

DATE REVISION: April 23, 2012

Name change from Identity Theft Prevention Policy

DATE UPDATE: July 23, 2018
DATE REVISION: October 25, 2021
November 26, 2024