LOWER YELLOWSTONE
RURAL ELECTRIC COOPERATIVE
Your Touchstone Energy® Cooperative

Date Adopted: 10/28/08
Date Revised: 1/24/17
Date Reviewed: 1/24/17

POLICY BULLETIN NO. 4

SUBJECT:

Identity Theft Prevention

OBJECTIVE:

A. To protect the identity/financial data of our member owners and minimize the possibility of identity theft of consumer information.

B. To establish a program to detect, prevent and mitigate identity theft.

PURPOSE:

To provide a guide in complying with the Federal Trade Commission "Red Flags" Rule.

POLICY:

A. As required by 16 CFR Part 1681, the cooperative will have and maintain a written "Identity Theft Prevention Program" plan.

B. The general manager and chief financial officer will be responsible for ongoing involvement in oversight, development, implementation and administrations of the Theft Prevention Program.

C. Training for the employees will be provided as necessary.

D. Oversight of third party providers will assure that they also comply with the program.

E. Periodically review and update the plan to reflect changes in risks to consumers and to the safety and soundness of the cooperative. A report will be made to the board of directors on compliance with the program and any incidents experienced for the year. The report will include:
   a. The effectiveness of the policies and procedures in addressing the risk of identity theft.
   b. Significant incidents that have occurred and managements' response.
   c. Recommendations for changing the program.

F. As risk factors are discovered, such as identity theft, member information breach, etc., the policy will be revised to address any future risks.

G. An investigation will be conducted when any of the following "Red Flags" are discovered.

   a. Incidents of identity theft.

   b. Methods of identity theft that reflect identity theft risk

c. Alerts, notifications, or other warnings received from a consumer reporting agency or service provider.
d. The presentation of suspicious documents such as altered or forged.
e. The presentation of suspicious personal identification information.
f. The unusual use of an account.
g. Notice from consumers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft.
h. A fraud or active duty alert is included with a consumer report.
i. A consumer reporting agency provides a notice of address discrepancy.
j. Identification photo that does not match the person.
k. Invalid social security number.
l. Mail sent to a consumer is frequently returned.

H. When signing up a new member or changing an address for an existing member, every effort must be made to verify the information given.

I. Monitoring the security of consumer identity data must be an ongoing process. When a consumer's information has been jeopardized, the following procedure should be followed:
   a. Contact the consumer.
   b. Eliminate the breach of information (such as change passwords, etc.).
   c. Notify law enforcement.

J. The general manager and chief financial officer will provide ongoing oversight of third party software providers and service providers that utilize consumer information to assure that consumer identity information is secure and utilized properly.

K. Require all employees to sign an "Employee Confidentiality Certification" by which those employees will not disclose confidential information to any unauthorized persons.

Identify Records. FTC requirements require us to first identify what records (covered accounts) we maintain or establish that could be "targets" for identity theft. It should be noted here that we are a rural electric **member-owned** cooperative. Our members are our owners. We have identified the following:

1. ***Social Security Numbers (SSN***). For many of our member accounts we establish, we have the member's social security number on file. If it is a joint account, we will have the SSN for either members or multiple SSNs if there are multiple names on the account. The SSNs are protected by internal security levels set up at the cooperative level. Only certain employees have access to "sensitive" member account information. The security levels are determined by management and implemented/maintained by the cooperative's system administrator. The software itself (what we call *Consumer Information Systems)* is purchased from a service provider called National Information Solutions Cooperative (NISC).

The software allows us to control the security levels via log-ins and passwords. Any reports generated with SSN fields have all but the last four digits of the member SSN "X"d out. The payroll software applications (also provided through NISC) have the same security level options as the CIS software.

2. ***Member Address Records.*** These records are maintained in much the same manner as the SSNs. LYREC has the option of setting the security levels. There is a lower security level with the address records as they are a critical part of our ability to provide service. As a provider of electricity (a service our U.S. Government has classified as critical or vital) we must have widespread access by our employees to member addresses and locations for emergency situations.

3. ***Credit Card Information.*** We allow payments of electric bills via credit card but we do not retain credit card information. We adhere to industry standard compliance for the handling of credit card transactions. Credit card payments are processed by approved 3rd party vendors.

4. ***Pay-By-Bank/ACH Payments.*** We do have bank account information (bank routing numbers and member bank account numbers) on file for members who pay their electric bill by automatically crediting their authorized bank accounts. LYREC have security levels set to allow only authorized employees access to those files. We also have bank information for employees so that their payroll checks can be automatically deposited into their bank account. Again, this is a different module than the CIS software and we also have strict security levels assigned for payroll/employee software applications. Currently that access is restricted to the general manager, chief financial officer and the plant accountant.

5. ***Personnel Files:*** Personnel files contain information such as social security numbers, bank deposit authorizations with bank account and bank routing numbers and pay rate information. These files are kept in a locked file cabinet located in a vault with limited personnel having access. Only authorized employees are able to access the file cabinet.

RED FLAG CATEGORIES: EXAMPLES

1. Alerts, notifications, or other warnings received from consumer reporting agencies or service providers, such as fraud detection services;
2. The presentation of suspicious documents;
3. The presentation of suspicious person identifying information, such as suspicious address change;
4. The unusual use of, or other suspicious activity related to a member account; and
5. Notice from customers, victims of identity theft; law enforcement authorities or other persons regarding possible identity theft in connection with member accounts held by Lower Yellowstone Rural Electric Cooperative.

GENERAL PRACTICES: COVERED ACCOUNTS. It seems pertinent at this point to briefly describe our current practices and what it takes to open an account to get service with Lower Yellowstone Rural Electric Cooperative. A new member must sign a membership application and pay the membership fee. The member must also agree to an Equifax credit report and, if required pay a security deposit. If a member declines the Equifax credit report the member must pay a security deposit that will be determined by the size of their service. LYREC allows members to sign up via phone. LYREC does not require photo ID.

We will provide training (both in-house and trying to arrange outside consultants via our state-wide organization) for our employees in identifying the "Red Flags" and what to do about it. This training will consist of the following:

A. Explain what the FTC "Red Flags" Rule is.
B. Review the types of records Lower Yellowstone Rural Electric Cooperative maintains that are primary identity theft targets (as noted above).
C. Review what our policies and procedures are with regards to preventing ID theft and what our appropriate response is to any "Red Flags."

RESPONSIBILITY:

The general manager is responsible for administering this policy and the recommending to the board any changes deemed desirable.