

TRI-COUNTY RURAL ELECTRIC COOPERATIVE, INC.

POLICY BULLETIN NO. 3-25

SUBJECT: IDENTITY THEFT PREVENTION PROGRAM

I. POLICY:

The purpose of this policy is to protect the identity/financial data of our member owners and minimize the possibility of identity theft of member information. This policy will comply with the requirements of the Federal Trade Commission and the “Red Flags” Rule. The policy will establish a program to detect, prevent and mitigate identity theft.

II. PROCEDURE:

- A. The Director of Financial Services will be responsible for on going involvement in oversight, development, implementation and administration of the Theft Prevention Program.
- B. Training for the employees will be provided as necessary.
- C. Oversight of third party software providers will assure that they also comply with the program. (Example – collection agencies)
- D. An annual report will be made or presented 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 management’s response
 - c. Recommendations for changing the program
- E. As risk factors are discovered, such as identity theft, a member information breach, etc., the policy will be revised to address any future risks.
- F. An investigation will be conducted when any of the following “Red Flags” are discovered:
 - 1. Alerts, notifications, or other warnings received from a consumer reporting agency or service provider
 - 2. Incidents of identity theft
 - 3. Methods of identity theft that reflect identity theft risks
 - 4. Documents provided for identification appearing altered or forged
 - 5. The presentation of suspicious personal identification information
 - 6. Photograph of ID inconsistent with appearance of member
 - 7. Information of ID inconsistent with information provided by person opening account

8. Information received not matching any address in consumer credit report, social security number has not been issued or appears on the social security administrations death master file, a file of information associated with social security numbers of those who are deceased
9. Personal identifying information associated with known fraud activity
10. Suspicious addresses supplied, such as a mail drop or prison, or phone number associated with pagers or answering services
11. Notice from consumers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft
12. The person opening the account is unable to supply identifying information in response to notifications that the application is incomplete
13. Mail sent to members repeatedly returned as undeliverable, despite on going transactions on active account
14. Financial institution or creditor notified that it has opened a fraudulent account for a person engaged in identity theft

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

H. Monitoring the security of member identity data must be an ongoing process. When a consumer's information has been jeopardized, the following procedure should be followed:

1. Contact the member
2. Eliminate the breach of information, such as change passwords, etc.
3. Notify law enforcement

I. The Director of Financial Services will provide on going oversight of third party software providers and service providers that utilize member information to assure that member identity information is secure and utilized properly.

III. RESPONSIBILITY:

President & CEO or Designee

Approved: April 14, 2009.
Reviewed: 11/20/09, 12/20/11.
Revised: