

Glacier Electric Cooperative, Inc.

Policy #424

IDENTITY THEFT PREVENTION PROGRAM

I. Objective:

To identify, mitigate and prevent identity theft by an existing member or applicant for new service with the Cooperative and to comply with Federal Trade Commission rules related to the implementation and monitoring of an Identity Theft Prevention Program.

II. Policy:

A. It shall be the policy of the Cooperative to comply with the requirements of the Federal Trade Commission, as outlined in 16 CFR Part 681.2, which states that any entity that offers a “covered account” shall establish an Identity Theft Prevention Program. Such program is established with a written policy and procedures.

B. The General Manager and Manager of Finance and Administration 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. Annually review the plan and update it periodically to reflect changes in risks to customers and to the safety and soundness of the Cooperative. An annual 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:

1. The effectiveness of the policies and procedures in addressing the risk of identity theft.
2. Significant incidents that have occurred and managements' response.
3. 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.

1. Incidents of identity theft
2. Methods of identity theft that reflect identity theft risks
3. Alerts, notifications, or other warnings received from a consumer reporting agency or service provider.
4. The presentation of suspicious documents, such as altered or forged.
5. The presentation of suspicious personal identification information
6. The unusual use of an account.
7. Notice from consumers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft.
8. A fraud or active duty alert is included with a consumer report
9. A consumer reporting agency provides a notice of address discrepancy
10. Identification photo that does not match the person
11. Invalid social security number
12. 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 should be made to verify the information given. Accounts are opened in person for the most part. A few are done by mail. Since the Cooperative is in a rural setting, the employees know many of the applicants or are able to obtain a credit reference from the

previous utility. Once the account information is in the computer, the employee needs a user ID and password to access the information.

I. Responses that the Cooperative deems appropriate to the Red Flags listed in Section G above may include the following:

1. Monitoring a utility account for evidence of identity theft;
2. Contacting the consumer;
3. Changing usernames and passwords, or other security devices used to access a utility account;
4. Reopening a utility account with a new account number;
5. Not opening a new utility account;
6. Closing an existing utility account;
7. Not attempting to collect on a utility account or not turning over a utility account to a collection agency;
8. Notifying law enforcement; or
9. Determining that no response is warranted under the particular circumstances.

J. The Cooperative will review the Program annually and update periodically as needed, based on the following factors:

1. The experiences of the Cooperative with identity theft;
2. Changes in methods of identity theft;
3. Changes in methods to detect, prevent, and mitigate identity theft;
4. Changes in the types of accounts that the Cooperative offers or maintains; and
5. Changes in the business arrangements of the Cooperative, including mergers, acquisitions, alliances, joint ventures, and service provider arrangements.

K. Oversight of this program will be the responsibility of the General Manager and Manager of Finance and Administration and shall include assigning responsibility for its implementation, preparing an annual report based on input from staff, and approving material changes to the Program as necessary to address changing identity theft risks. Staff training will be provided as necessary to effectively implement the Program.

L. Staff responsible for implementation should report to the General Manager and Manager of Finance and Administration at least annually on compliance by the Cooperative with Section 681.2. The report should evaluate issues such as:

1. The effectiveness of the policies and procedures of the Cooperative;
2. Service provider arrangements;
3. Significant incidents involving identity theft and management's response; and
4. Recommendations for material changes to the Program.

M. Whenever the Cooperative should engage a service provider to perform an activity in connection with one or more of the utility accounts, the Cooperative will take steps to ensure that the activity of the service provider is conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft.

N. All employees must follow Policy 420 dealing with confidentiality of information.

Approved:

October 29, 2008

President: Lee Holden