CLEARWATER POWER COMPANY
Lewiston, Idaho 83501

POLICY BULLETIN NO. 140A

SUBJECT: Identity Theft Prevention

POLICY:

The purpose of this policy is to establish a program to detect, prevent, and mitigate Identity Theft by protecting the identity and financial data of our Members and minimizing the possibility of Identity Theft of Member information in compliance with the Fair and Accurate Credit Transaction Act of 2003 as amended (as set forth in Federal Register publication – 16 CFR Part 681).

RESPONSIBILITY:

General Manager, Manager of Member Services, Manager of Engineering, Director of Member Services, Director of Information Systems, and Engineering and Member Services Personnel

PROCEDURE:

I. DEFINITIONS

Covered Account: A Member's account that the Cooperative offers or maintains and involves multiple payments or transactions. A Covered Account may also include any other account which there is a reasonably foreseeable risk to Members or the safety and soundness of the Cooperative to Identity Theft, including financial, operational, compliance, reputation, or litigation risks.

Identity Theft: A fraud committed or attempted use of the identifying information of another person without authority.

Red Flag: A pattern, practice, or specific activity that indicates the possible existence of Identity Theft. Specific descriptions of Red Flags applicable to this policy are set forth below.

II. IDENTIFICATION OF RELEVANT RED FLAGS

Considering the methods by which the Cooperative establishes and opens accounts, provides access to account information, and past experience the Cooperative has with Identity Theft, the events and/or occurrences set forth below reasonably indicate the potential for Identity Theft and should be considered Red Flags:

(A) Alerts, Notifications, or Other Warnings Received from Consumer Reporting Agencies or Service Providers, Such as Fraud Detection Services.

Although it is not common practice for the Cooperative to request or receive consumer reports, the following should be considered Red Flags in any case where the Cooperative requests or receives such reports:

1. A fraud or active duty alert is included with a credit report.

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

3. A credit reporting agency provides a notice of address discrepancy.

4. 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:

    a. A recent and significant increase in the volume of inquiries;
    b. An unusual number of recently established credit relationships;
    c. A material change in the use of credit, especially with respect to recently established credit relationships; or
    d. An account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor.

(B) The Presentation of Suspicious Documents.

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

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

3. Other information on the identification is not consistent with information provided by the person opening a new Covered Account or Member presenting the identification.

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

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

(C) The Presentation of Suspicious Personal Identifying Information or Suspicious Address Changes.

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

   a. Information on a letter of credit does not match personal information provided; or
   b. The Social Security Number (SSN) has not been issued, or is listed on the Social Security Administration's Death Master File.

2. Personal identifying information provided by the Member is not consistent with other personal identifying information provided by the Member.

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

   a. The address on an application is the same as the address provided on a fraudulent application; or
   b. The phone number on an application is the same as the number provided on a fraudulent application.

4. 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:

   a. The address on an application is fictitious, a mail drop, or a prison; or
   b. The phone number is invalid, or is associated with a pager or answering service.

5. The SSN provided is the same as that submitted by other persons opening an account or other Members.

6. 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.

7. 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.

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

9. If the Cooperative uses challenge questions, the person opening the Covered Account or the Member cannot provide authenticating information beyond that which generally would be available from a wallet or credit report.

(D) Unusual Use of, or Other Suspicious Activity Related to, a Covered Account.

1. Shortly following the notice of a change of address for a Covered Account, the Cooperative receives a request for refund of a credit balance or deposit.

2. A Covered Account that has been inactive for a reasonably lengthy period of time is used (taking into consideration the type of account, the expected pattern of usage and other relevant factors).

3. Mail sent to the Member is returned repeatedly as undeliverable although electric usage continues in connection with the Member's Covered Account.

4. The Cooperative is notified that the Member is not receiving paper account statements.

5. The Cooperative is notified of unauthorized usage in connection with a Member's Covered Account.

(E) Notice from Members, Victims of Identity Theft, Law Enforcement Authorities, or Other Persons Regarding Possible Identity Theft in Connection with Covered Accounts Held by the Cooperative.

1. The Cooperative is notified by a Member, a victim of Identity Theft, a law enforcement authority, or any other person that the Cooperative has opened a fraudulent account for a person engaged in Identity Theft.

III. DETECTION

In an effort to detect Red Flags, the Cooperative shall obtain and maintain information from Members and potential Members that apply for electric service.

In the case of existing Covered Accounts, the Cooperative shall monitor transactions and verify Member access to Covered Accounts by using information obtained upon application for electric service.

IV. PREVENTING AND MITIGATING IDENTITY THEFT

In the event a Red Flag is detected, the Cooperative shall assess the degree of risk posed including any aggravating circumstance(s) that may heighten the risk of Identity Theft. After assessing the degree of risk posed, the Cooperative shall respond to the Red Flag in an appropriate manner, which may include the following:

(A) Monitoring a Covered Account for evidence of Identity Theft;
(B) Contacting the Member;
(C) Changing security access or requiring additional information to permit access to a Covered Account;
(D) Reopening a Covered Account with a new account number;
(E) Not opening a new Covered Account;
(F) Closing an existing Covered Account;
(G) Not attempting to collect on a Covered Account or not selling a Covered Account to a debt collector;
(H) Notifying law enforcement; or
(I) Determining that no response is warranted under the particular circumstances.

Service providers hired by the Cooperative to perform any activity in connection with any Covered Account must take appropriate steps to prevent Identity Theft and must have implemented and follow a similar Identity Theft prevention program.

V. UPDATING THE PROGRAM

The Cooperative shall periodically reassess the Program (including the Red Flags determined to be relevant) to reflect changes in risk to Members or to the safety and soundness of the Cooperative from Identity Theft. The reassessment should be done no less than annually based on factors such as:

(A) The Cooperative's past experience(s) with Identity Theft;
(B) Changes in methods of Identity Theft;
(C) Changes in methods to detect, prevent, and mitigate Identity Theft;
(D) Changes in the types of accounts that the Cooperative offers or maintains; and

(E) Changes in the business arrangements of the Cooperative, including mergers, acquisitions, alliances, joint ventures, and service provider arrangements.

VI. PROGRAM ADMINISTRATION

(A) The Manager of Member Services shall be responsible for reporting Program compliance annually to the Board of Directors, which shall include the following:

1. The effectiveness of the Program in addressing the risk of Identity Theft in connection with the opening of Covered Accounts and with respect to existing Covered Accounts;
2. Material Program matters related to service provider arrangements;
3. Significant incidents involving Identity Theft and management's response; and
4. Recommendations for material changes to the Program.

(B) The Manager of Member Services shall oversee training, report preparation, and program implementation (including detecting Red Flags and preventing and mitigating Identity Theft).

SOURCE: Adopted by Board Resolution – October 16, 2008.
Amended in Part – November 24, 2015.
Board Reviewed – January 20, 2010; January 19, 2011; January 18, 2012; January 16, 2013; January 22, 2014; January 20, 2015.