DCEC
Delaware County
Electric Cooperative

POLICY

SUBJECT: Identity Theft Red Flag Prevention

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 – commonly known as "Identity Theft". In order to carry out that policy, the Cooperative hereby adopts the following policy for identifying or detecting Red Flags that should raise concerns for the Cooperative that a member's information is potentially being misused or stolen.

PROCEDURE:

I. DEFINITIONS

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

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

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.

II. POLICY RATIONALE

Under federal law and regulations, the Cooperative is required to adopt an Identity Theft Red Flag Prevention policy under the Federal Trade Commission ("FTC") regulations at 16 C.F.R. § 681.2 *et seq.*

III. IDENTIFICATION OF ACCOUNTS SUBJECT TO THE POLICY

The Cooperative maintains accounts for its members that allow the members to pay for service after it has been rendered. Bills are sent and payments are due on a monthly basis. These accounts are covered by this Red Flag policy.

IV. IDENTIFICATION AND DETECTION OF POTENTIAL RED FLAGS

A. Risk Factors. In identifying potential Red Flags associated with the accounts that the Cooperative maintains, the Cooperative considers the following Identity Theft risk factors:

1. Types of Covered Accounts. The Cooperative is an electric Cooperative serving rural New York State, providing its members with electric utility service. The Cooperative serves approximately 5400 members. Turnover in members is low, as is the number of address change requests received from members. Payments from members for services rendered are due by the 12th day of the month following the billing date. The Cooperative does not 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.

2. Methods for Opening Accounts.

   a. Prospective Member Appears in Person at Cooperative's Office: The Cooperative requires that prospective members who wish to receive utility service submit a membership application with the following information: (1) name and date of birth of the prospective member; (2) address location where service shall be provided; (3) billing address; (4) home phone number; (5) cell phone number if available; (6) e-mail address if available; (7) closest living relative; and (8) at the prospective member's option, Social Security Number or Tax Identification Number. If a member declines to provide their social security number they are not denied service but they are subject to the maximum deposit per the Cooperative's Deposits Policy. The applicant must also present to the Member Service Representative a valid Government issued photo identification as proof of identity.

   b. Prospective Member Does Not Appear in Person at Cooperative's Office: The Cooperative requires that prospective members who wish to receive utility service submit a membership application with the following information: (1) name and date of birth of the prospective member; (2) address location where service shall be provided; (3) billing address; (4) home phone number; (5) cell phone number if available; (6) e-mail address if available; (7) closest living relative; and (8) at the prospective member's option, Social Security Number or Tax Identification Number. If a member declines to provide their social security number they are not denied service but they are subject to the maximum deposit per the Cooperative's Deposits Policy and they are required to appear in person at the

Cooperative's office and provide a government issued photo ID. See the previous paragraph for more details.

3. Methods for Accessing Account Balance, Payment Information and Disconnect Notices. The Cooperative allows members and third parties designated by members in writing to access their account balances, payment information, and disconnect notices using the following methods:

   (a) in person at the Cooperative's offices after providing their name and account number or their name and address;

   (b) over the telephone after providing the Cooperative's employees their name and account number or their name and address; or

   (c) over the Internet using a secure password.

[Is providing the address and account number our security check here? No other method of identification required?]

4. Methods for Accessing Member Information Other Than Account Balance, Payment Information, and Disconnect Notices. The Cooperative allows members to access their information other than account balance, payment information, and disconnect notices using the following methods:

   (a) in person at the Cooperative's offices with a picture identification or after providing their name, address and social security number or after providing their name, address and birth date;

   (b) over the telephone after providing the Cooperative's employees with their name, address and social security number or after providing their name, address and birth date; or

   (c) over the Internet using a secure password.

5. 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' personal identifying information. Given the limited amount and types of services and credit provided to its members, the small size of the population it serves, and the relatively low rate of change in membership, coupled with the Cooperative's policies for securing members' personal information,

the Cooperative believes the risk of its members being the subject of Identity Theft through the information collected by the Cooperative to be low.

B. Sources of Red Flags. In identifying potential Red Flags associated with the accounts that the Cooperative maintains, the following sources of Red Flags for Identity Theft have been identified:

1. Past Incidents of Identity Theft. 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 utility. In the event of incidents of Identity Theft in the future, such incidents shall be used to identify additional Red Flags and added to this policy.

2. Identified Changes in Identity Theft Risk. As provided in Section VI below, the Cooperative will review this policy from time to time, 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, the Cooperative will review additional regulatory guidance from the FTC and other consumer protection authorities.

C. Categories of Red Flags. In identifying potential Red Flags associated with its accounts, the Cooperative has considered the following categories of Red Flags for Identity Theft:

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.

Required Response. If a staff member receives an alert, notification, or other warning from a consumer reporting agency, the staff member shall immediately notify the General Manager. In some cases when the identity of a prospective member is in doubt, services may be denied until the discrepancy can be resolved.

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

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

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

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

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

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

Required Response. Member Service Representatives and other personnel of the Cooperative shall report to the General Manager 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 the General Manager'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 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 address or telephone number submitted by an unusually large number of other persons opening accounts or other members.

(g) 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.

Required Response. 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. The Cooperative is not to provide account information without first clearing any discrepancies in the information provided.

4. Notices. Notice from members, victims of Identity Theft, law enforcement authorities, or other persons regarding possible Identity Theft in connection with member accounts can also be a Red Flag for Identity Theft.

   Required Response: 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.

5. Suspicious Account Activity. Marked changes in usage or deviation from expected usage patterns such as may be evident to a staff member in the normal course of reviewing billing exception reports or transformer loading reports.

   Required Response: Cooperative staff members shall be trained to recognize suspicious usage patterns such as extremely high usage. Upon discovery of suspicious usage patterns, the member shall be notified of the suspicious usage pattern.

V. PREVENTING AND MITIGATING IDENTIFY THEFT

A. If the Cooperative discovers that any of its members have become a victim of Identity Theft through personal information used by the utility in opening or maintaining a member's account, management shall take appropriate steps that it deems necessary 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 law enforcement; or

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

B. The Cooperative has a business relationship with National Information Solutions Cooperative (NISC), a third-party application service provider (ASP) for the Cooperative's consumer information system (CIS) database. Under this business relationship, NISC has access to member information covered under this Policy. The General Manager shall ensure that NISC's work for the Cooperative is consistent with this policy by (a) amending the contract to incorporate these requirements; or (b) by determining that NISC has reasonable alternative safeguards that provide the same or a greater level of protection for member information as provided by the Cooperative.

C. The Cooperative has a business relationship with On-Line Utility Exchange, a third-party credit risk service provider. Under this business relationship, On-Line Utility Exchange has access to member information covered under this Policy. The General Manager shall ensure that On-Line Utility Exchange's work for the Cooperative is consistent with this policy by (a) amending the contract to incorporate these requirements; or (b) by determining that On-Line Utility Exchange has reasonable alternative safeguards that provide the same or a greater level of protection for member information as provided by the Cooperative.

VI. Updating and Administering the Policy

A. The Cooperative shall consider updating this policy to determine whether it has experienced any Identity Theft of its members' accounts, whether changes in the methods of Identity Theft require updating to this Policy, or whether changes are necessary to detect, prevent, and mitigate Identity Theft. Management will continue to monitor changes in methods of Identity Theft, and re-evaluate this Policy in light of those changes.

B. Administration of the Policy shall be as follows:

1. The Board of Directors has adopted this Policy and will have ultimate oversight of this Policy, but the Policy shall be managed by General Manager of the Cooperative. The General Manager shall have authority to delegate oversight and compliance to other individuals at the senior level management level.

2. Potential changes to the Policy shall be reviewed at least annually by the General Manager. The General Manager shall bring proposed changes to the Policy to the Board of Directors, who have the sole authority to modify the Policy.

3. Reports.

(a) The General Manager shall prepare a report, at least annually, regarding the implementation and progress of the utility's Policy for review by the Board of Directors.

(b) The above-described report 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 General Manager shall keep records of meetings regarding this Policy showing the dates and topics discussed. The General Manager shall also cause to be maintained a file with copies of the most recent annual reports prepared under the Policy.

RESPONSIBILITY: The General Manager and the Board of Directors.

DELAWARE COUNTY ELECTRIC COOPERATIVE, INC.

Approved by Board of Directors	Oct 26, 2010
Revised by Board of Directors	December 18, 2013
Revised by the Board of Directors	February 25, 2014
Revised by the Board of Directors	December 22, 2015
Revised by the Board of Directors	December 19, 2017