M. J. M. ELECTRIC COOPERATIVE, INC.

SECTION III- MEMBERS AND CONSUMERS
Policy 10 APPROVED: 10/23/2008

REVISED: 08/27/2015 12/21/2018 12/23/2020

IDENTITY THEFT PREVENTION

I. OBJECTIVE

The purpose of this policy is to:

A. Create an identity theft prevention program (Identity Theft Prevention Program) that ensures the privacy and accuracy of Member/Consumer credit report information, reduces the incidence of identity theft and aids victims of identity theft by implementing standards of care and procedures allowing the detection, prevention and mitigation of identity theft when using member/consumer personal information within the possession of the Cooperative.

B. Establish procedures to identify and respond to risk factors called "Red Flags" to detect, prevent and mitigate identity theft from the Cooperative's Member/Consumer personal information.

C. Implement procedures for responding appropriately to evidence of identity theft and unauthorized use of Member/Consumer personal information.

D. Provide for staff training and periodic review and updating of the Identity Theft Prevention Program.

E. Provide for oversight, implementation and administration of the Identity Theft Prevention Program by the Cooperative's Management and governing Board of Directors.

F. Identify the proper purposes for which customer consumer reports, or credit information obtained from Consumer Reporting Agencies, may be used by the Cooperative.

G. Comply with the Fair Credit Reporting Act of 1970, 15 U.S.C. Section 1681et. seq. (FCRA), the Fair and Accurate Credit Transactions Act of 2003, 15 U.S.C. Section 605(h)(s) (FACT Act) and the Identity Theft Red Flag rules promulgates by the Federal Trade Commission on November 9, 2007 and found at 16 CFR Part 681.

II CONTENT

A. DEFINITIONS

1. "**Consumer Report**" is defined as any written, oral or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics or mode of living which will be used at least partly to determine the consumer's eligibility to receiver and pay for services. Consumer Reports are commonly known as credit reports.

2. "**Consumer Reporting Agency**" (CRA) is defined as any person which, regularly engages in assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties. Examples include Equifax, TransUnion and Experian.

3. "**Covered Account**" means a utility account primarily for personal family or household purposes and may include small business sole proprietor accounts where there is a reasonably foreseeable risk of identity theft.

4. "**Red Flags**" as used herein are patterns, practices or specific activities that taken together or alone, indicate the possible occurrence of identity theft, including the following:

    a. Alerts, notifications, or other warnings received from CRAs or other service providers, such as fraud detection services, which include:

        i. Fraud or active duty alert;
        ii. Credit freeze notice; or
        iii. Address discrepancy notice informing of a substantial difference between the address provided by the consumer and the address on file with the CRA.
        iv. Inconsistent pattern of activity based on history and pattern of activity, such as recent and significant increase in volume of inquiries, unusual number of recently established credit relationships, a material change in the use of credit or an account that was closed for cause or abuse.

    b. The presentation of suspicious documents. For example:

        i. The application or identification documents appear to be altered or forged;
        ii. The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer;
        iii. The documents are inconsistent with information provided by the customer; or
        iv. The documents are inconsistent with readily accessible information on file with the Cooperative.

c. The presentation of suspicious personal identifying information, such as when:

i. The personal identifying information is inconsistent when compared to other information on file with the Cooperative, from the Member/Consumer, or from external information sources (e.g., address discrepancies and un-issued Social Security Number (SSN), or the date of birth does not match the corresponding SSN range).
ii. The Member/Consumer fails to provide all required personal information on an application or in response to notification that the application is incomplete.
iii. The personal identifying information matches that of known fraudulent activities.
iv. The personal identifying information is of a type commonly associated with fraudulent activity, such as invalid phone number, mail drop or prison address.
v. The address or telephone number is used by unusually large number of persons opening accounts.

d. The unusual use of, or other suspicious activity related to, a Covered Account, such as:

i. With a new Covered Account, the Member/Consumer fails to make the first payment or makes an initial payment but no subsequent payments.
ii. A Member/Consumer with a Covered Account notifies the Cooperative that he or she is not receiving paper account statements.
iii. The Cooperative is notified of unauthorized services in connection with a Member/Consumer's Covered Account.
iv. A Covered Account is used in a manner that is inconsistent with established patterns of activity on the account (e.g. nontypical activity in bill payment).
v. 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).
vi. Repeated returned mail even though the Member/Consumer with a Covered Account continues to receive electric service.

e. Notice from Member/Consumers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with Covered Accounts held by the Cooperative.

B. DUTIES TO DETECT, PREVENT AND MITIGATE

1. GENERAL

a. All MJM card payment devices shall be physically inspected at the beginning of each business day by designated Employees using said devices. Any

evidence of physical tampering shall be reported to the IT Administrator or Management and the device will be taken offline for further investigation. Properly trained and authorized Employees may use the Cooperative approved point of sale devices **(currently MX 925 and P200)**.

b. All Employees authorized and trained to take payments may not transmit the PAN (personal account number), also referred to as credit card number, through any email or messaging systems.

c. All Employees who engage in remote support sessions must deactivate remote access after a support session has ended.

d. All Employees using personal devices with company data must remove all company data from said device before removing said device from their ownership. Employees are also directed to notify the IT Administrator or Management when a personal device with company data on it has been removed from their possession.

e. All Employees that have access to information in a Covered Account shall be trained to detect, and respond to, Red Flags.

f. Means of identity verification shall include any one or more of the following:

i. Applicant's full name
ii. Mailing address;
iii. Street Address;
iv. Phone number;
v. Government-issued Photo identification;
vi. Passwords (whether assigned by the Cooperative or user-defined)
vii. For an individual, date of birth;
viii. For a U.S. person, a taxpayer identification number;
ix. For a non-U.S. person, one or more of the following:
    1. Taxpayer identification number; passport number and country of issuance;
    2. Alien identification card number; or
    3. Number and country of issuance of any other government-issued document evidencing nationality or residence and bearing a photograph or similar safeguard.

2. <u>New Accounts</u>

a. When opening new Covered Accounts and performing other functions regarding Covered Accounts including but not limited to address and billing changes, the identity of the applicant or Member/Consumer shall be verified to the extent reasonable and practicable under the circumstances.

b. The Cooperative should not open a new Covered Account if there is a fraud or active duty alert for the applicant or Member/Consumer unless the

Cooperative gathers additional information sufficient to form a reasonable belief that the user knows the identity of the applicant or Member/Consumer making the request.

c. If one or more Red Flags are detected during the application process for a Covered Account, while servicing a Covered Account, or otherwise, the staff member shall notify a Supervisor or other Management level staff of the detention.

3. Existing Accounts

a. When servicing Covered Accounts, such as processing change of address requests, staff shall authenticate the identity of the Member/Consumer as well as verify the change of address or other information on the account.

b. The Cooperative should not open a new Covered Account or make material changes to an existing Covered Account if there is a fraud or active duty alert for the applicant or Member/Consumer unless the Cooperative gathers additional information sufficient or form a reasonable belief that the user knows the identity of the applicant or Member/Consumer making the request.

c. If one or more Red Flags are detected while servicing a Covered Account, or otherwise, the staff member shall notify their Supervisor or other Management level staff of the detection.

d. The Cooperative will flag or mark Covered Accounts that are to be monitored so that any reviewer (e.g. Customer Service Representative, hereinafter "CSR") servicing the account can be aware for the previous Red Flags or other concerns.

4. Supervisor Actions

a. Employees who are notified of a Red Flag shall evaluate the degree of risk posed by the particular Red Flag(s).

b. In determining an appropriate response, any aggravating factors, such as additional known Red Flags increase the risk of identity theft should be considered.

c. Appropriate responses to a Red Flag may include the following:

i. Monitoring the Covered Account for evidence of identity theft;
    1. The Cooperative will mark accounts in such a manner so as to make it known to the CSR or other employee reviewing this account of any previous Red Flag concerns.
ii. Contacting the Consumer/Member;
iii. Changing any passwords, security codes, or other security devices that permit access to the Covered Account;

iv. Reopening the Covered Account with a new account number;
v. Not opening a new Covered Account;
vi. Closing an existing Covered Account;
vii. Not attempting to collect on a Covered Account or not referring a Covered Account to a debt collector;
viii. Notifying law enforcement; or
ix. Determining that no response is warranted under the particular circumstances.

5. Record Management

a. The Cooperative shall maintain records of the information used to verify the applicant's identity, including name, address and other identifying information as applicable and used by the Cooperative to verify a person's identity.

b. If a governmental agency provides the Cooperative with a list of known or suspected terrorists, the Cooperative shall consult such list to determine whether the applicant appears on such list.

C. SERVICE PROVIDERS

1. If the Cooperative engages a service provider to perform an activity in connection with one of more Covered Accounts, the Cooperative shall take steps to ensure that such activity is conducted according to reasonable policies and procedures designed to detect, prevent and mitigate the risk of identity theft.

2. Where appropriate, the Cooperative shall require by contract that service providers have policies and procedures to detect relevant Red Flags that may arise during performance of the services, and to either report the occurrence of the Red Flags to the Cooperative or to take appropriate steps to prevent or mitigate identity theft.

D. CONSUMER REPORTS

1. Use of Consumer Reports. Consumer Reports shall be used only in connection with the extension of credit, the extension of or provision of services to a Member/Consumer, to review an account to determine if the Member/Consumer meets the terms of the account and for such other legitimate Cooperative purposes as may be approved by Cooperative Management.

2. Notice of Adverse Actions. If the Cooperative takes an adverse action based on a Consumer Report, then the Cooperative shall provide written notice either via in person, U.S. Mail or electronic notice (e.g. email) to the applicant, which shall include notice of the adverse action; the name, address and toll-free telephone number of the CRA that provided such report; a statement that the CRA did not make the decision to take adverse action and is

unable to provide the Member/Consumer with specific reasons why the action was taken; and notice of the Member/Consumer's right to obtain a free copy of such report from the CRA within 60 days and to dispute the accuracy or completeness of such report, as required by applicable federal Consumer Credit Protection laws (15 U.S.C.A. §§ 1681m and 1681j).

3. Notice of Address Discrepancy.

    a. If the Cooperative receives a notice of address discrepancy from a CRA, the Cooperative must reasonably confirm the identity and address of the applicant.
    b. The Employee receiving the notice of address discrepancy shall report the notice to a Supervisor or other Management level staff.
    c. Employees who are notified of the notice of address discrepancy shall take reasonable steps to verify the identity of the applicant by verifying the information provided by the CRA with the Member/Consumer or comparing other information maintained by the Co-op about the Member/Consumer (e.g. change of address notification, account records, service applications, etc.).
    d. If the Cooperative obtains adequate confirmation to form a reasonable belief that the applicant is the same person listed in the notice of address discrepancy (Consumer Report), then the Cooperative shall document how it resolved the address discrepancy and may proceed to open the account or to take the requested action.
    e. If the Cooperative is unable to form such a reasonable belief regarding the identity of the applicant, then the Cooperative shall respond appropriately under the circumstances, such as not opening an account for the applicant, closing an existing account, or taking other actions as determined appropriate based on the circumstances.

E. FURNISHING INFORMATION

1. When furnishing information to a CRA, the Cooperative shall; report accurate information; correct and update incomplete or inaccurate information; report accounts closed voluntarily by the Member/Consumer; and report delinquent accounts that have been placed for collection, charged to profit or loss or subject to a similar action.

2. The Cooperative shall not furnish information to a CRA if the furnisher has reasonable cause to believe such information is inaccurate.

F. UPDATE AND COMPLIANCE REPORTS

1. The Identity Theft Prevention Program and the defined Red Flags should be reviewed and updated periodically based upon the following:

    a. Experiences of the Cooperative 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 Cooperative's business arrangements which would impact the Identity Theft Prevention Program, such as service provider arrangements.

2. Employees responsible for implementation of the Identity Theft Prevention Program shall provide compliance reports at least annually to the President/CEO or other Management regarding the Cooperative's compliance with applicable law.

3. The President/CEO or other Management shall review the compliance reports and take appropriate action, if required.

4. Compliance reports should address material matters related to the Identity Theft Prevention Program and evaluate issues such as:

   a. The effectiveness of the Cooperative's policies and procedures;
   b. Service provider arrangements;
   c. Significant incidents involving identity theft and Management's response, and
   d. Recommendations for material changes to the Identity Theft Prevention Program.

G. SOCIAL SECURITY NUMBERS

1. The Cooperative shall not require Member/Consumers to transmit a Social Security Number via the Internet unless the transmission is secure or encrypted.

2. The Cooperative shall not require Member/Consumers to use Social Security Number to access its website unless coupled with a Personal Identification Number or other method of identification.

3. The Cooperative may require a Social Security Number to establish or terminate an account, to contract services, or to confirm the accuracy of a Social Security Number on file.

4. The Cooperative may use Social Security Numbers for internal administrative or verification purposes.

III. RESPONSIBILITY

A. The President/CEO or other Management shall be responsible for implementation, administration and review of the Identity Theft Prevention Program.

B. The President/CEO or other Management may suggest changes to the Identity Theft Prevention Program and guidelines, as necessary to address changing identity theft risks, for the Board's review and consideration.

C. The President/CEO or other Management may assign the specific responsibility of implementation to members of the staff of the Cooperative.

D. The President/CEO or other Management shall oversee applicable service provider arrangements and staff training as necessary to facilitate effective implementation and oversight of service providers.

William R Heyen, Secretary

ADOPTED: 10/23/2008

EFFECTIVE: November 1, 2008