Holy Cross Energy
Corporate Policies

Identity Theft Prevention
Policy Number: 2.4
Original Effective Date: November 18, 2015
Revised Dates: May 18, 2022

1. OBJECTIVE

1.1 To establish an identity theft protection policy as required by Federal law and regulations.

2. POLICY

2.1 It shall be the policy of Holy Cross Electric Association, Inc., a/k/a Holy Cross Energy ("Holy Cross"), to take all reasonable steps to identify, detect and prevent the theft of its members' personal information.

2.2 Definitions.

2.2.1 The terms "Personally Identifiable Information" or "PII" mean 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 drivers' license or identification number, alien registration number, government passport number, employer or taxpayer identification number or address.

2.2.2 The term "Identity Theft" means a fraud committed or attempted using the PII of another person.

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

2.2.4 The terms "member" or "members" for purposes of this Policy include both members of Holy Cross and to the extent Holy Cross has non-member patrons, the non-member patrons of Holy Cross.

2.3 Employee Use of Data. Holy Cross employees need access to certain member information located within the member information system, billing software and storage files. Names, addresses and electric service billing information are available to those Holy Cross employees who have access to such software.

2.4 Covered Accounts. Holy Cross is an electric cooperative serving portions of Eagle, Garfield, Pitkin, Mesa and Gunnison Counties, all in the State of Colorado, providing its members with electric utility service. Member accounts can consist of one or more different components, each subject to Identity Theft risk factors as described below:

2.4.1 Payments for Electric Service Rendered. Payments from members for services rendered are due within 15 days of billing. Holy Cross does not regularly provide credit to its members beyond this revolving, monthly account for utility service. Such service is rendered at a fixed physical location known to Holy Cross. As a result, there is a low risk of misuse of PII to perpetrate fraud on Holy Cross for utility services rendered. However, PII maintained by Holy Cross could be used to perpetrate Identity Theft and defraud other businesses if the information was wrongfully altered or disclosed.

2.4.2 Payments for Line Extensions. For some line extensions, members may have the option of paying off the costs of the extension over time through their electric bills. Line extensions are constructed at a fixed physical location known to Holy Cross. As a result, there is a low risk of misuse of PII to perpetrate fraud on Holy Cross for line extensions that are paid for over time.

However, PII maintained by Holy Cross could be used to perpetrate Identity Theft and defraud other businesses if the information was wrongfully altered or disclosed.

2.4.3 Utility Deposits. For some members, utility deposits are required prior to the initiation of service or additional deposits may be required. These deposits are held under the terms and conditions of Holy Cross rules and regulations and may eventually be refunded to the member. There is some risk that a member who is a victim of Identity Theft could have the member's utility deposit refunded to an identity thief. Additionally, PII maintained by Holy Cross could be used to perpetrate Identity Theft and defraud other businesses if the information was wrongfully altered or disclosed.

2.4.4 Capital Credit Accounts. All members are eligible for allocation of capital credits, also known as member equity, in accordance with Holy Cross's Bylaws and Corporate Policies ("Corporate Policy" or "Policy"). Capital credits are retired in accordance with the Bylaws and Policies, either in the form of a check to the member or a credit on the member's bill. There is some risk that a member who is a victim of Identity Theft could have the member's capital credit retirement check sent to an identity thief. Additionally, PII maintained by Holy Cross could be used to perpetrate Identity Theft and defraud other businesses if the information was wrongfully altered or disclosed.

2.5 Methods for Opening Accounts. Holy Cross requires that prospective members who wish to receive utility service provide the following information: (1) name and date of birth of adult household members on the account; (2) personal password; (3) address location where service shall be provided; (4) contact and billing information including mobile phone number; (5) e-mail address; and (6) employer identification number, for business accounts.

2.6 Methods for Accessing Accounts. Holy Cross shall provide members access to their account information only after verifying the member's identity using one of the following methods:

2.6.1 In person at Holy Cross's offices with acceptable identification;

2.6.2 Over the telephone after providing Holy Cross's Member Service Representative ("MSR") with confirmation of certain PII, such as the caller's date of birth and/or the address and telephone number of the service location, employer identification number for a business, connect date of service in question or amount of last bill in question; or

2.6.3 Over the internet using a secure password for payment options or customer care verified by an MSR or through Holy Cross' SmartHub app.

2.7 Previous Experience with Identity Theft. As of the Revised Date of this Policy, Holy Cross is not aware of any security breach of, or unauthorized access to, its systems that are used to store members' PII.

2.8 Sources of Red Flags. In identifying potential Red Flags associated with the accounts that Holy Cross maintains, Holy Cross's Board and management have considered the following sources of Red Flags of Identity Theft:

2.8.1 Past Incidents of Identity Theft. As described above, Holy Cross is not aware of any security breach of, or unauthorized access to, its systems that are used to store members' personal Identifying Information. In the event of incidents of Identity Theft in the future, such incidents shall be used to identify additional Red Flags and this Policy will be amended accordingly.

2.8.2 Identified Changes in Identity Theft Risk. Holy Cross will continually review this Policy, Holy Cross's operations and Holy Cross's experience with Identity Theft for changes in Identity Theft risk.

2.8.3 Applicable Supervisory Guidance. In addition to considering the guidelines initially published with the Federal Trade Commission's ("FTC") Red Flag regulations, as a part of its continual review, Holy Cross will review additional regulatory guidance from the FTC and other

consumer protection authorities as it is made available to Holy Cross. This review shall focus on new Identity Theft risks and recommended practices for identifying, detecting, and preventing Identify Theft.

2.9 Categories of Red Flags. In identifying potential Red Flags associated with the accounts that Holy Cross maintains, Holy Cross's Board and management have considered the following categories of Red Flags for Identity Theft and will take the following actions upon discovering such Red Flags:

2.9.1 Alerts, Notifications and Warnings. Holy Cross does not generally apply for or receive consumer reports related to its members. For this reason, Holy Cross does not anticipate receiving any consumer reports that might alert it to potential Identity Theft related to a member. However, if Holy Cross does receive such a report, MSRs shall report such activity to a supervisor for further review and inquiry.

2.9.2 Suspicious Documents. The presentation of suspicious documents can be a Red Flag for Identity Theft. Presentation of suspicious documents includes:

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

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

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

2.9.2.4 Other information on the identification is not consistent with readily accessible information that is on file with Holy Cross.

MSRs and other Holy Cross personnel shall notify their supervisor 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 a supervisor's attention immediately if any member presents an invalid identification, or identification that appears forged for the purpose of obtaining access to account information.

2.9.3 Suspicious PII. The presentation of suspicious PII, such as a suspicious address change, can be a Red Flag for Identity Theft. Presentation of suspicious PII occurs when:

2.9.3.1 PII provided by the member is not consistent with other PII provided by the member, for example: there is a mismatch between service location name and address vs. billing name and address.

2.9.3.2 PII provided by the member is associated with known fraudulent activity as indicated by internal or third party sources used by Holy Cross, for example: the address or phone number on an application is the same as the address or phone number provided on a known fraudulent application.

2.9.3.3 PII provided by the member is of a type commonly associated with fraudulent activity as indicated by internal or third party sources used by Holy Cross, for example: the address on an application is fictitious, a mail drop or a prison; or the phone number is invalid, or is associated with a pager or answering service.

2.9.3.4 The address or telephone number provided is the same as that of other members or similar to the account number or telephone number submitted by an unusually large number of other persons opening accounts.

2.9.3.5 The person opening the covered account or the member fails to provide all required PII on an application or in response to notification that the application is incomplete.

2.9.3.6 PII provided by the member is not consistent with PII that is on file with Holy Cross.

MSRs shall notify their supervisor 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. Holy Cross is not to provide account information without first clearing any discrepancies in the information provided.

2.9.4 Suspicious Activity. The unusual use of, or other suspicious activity related to, a member account is also a Red Flag for potential Identity Theft. Suspicious activities include:

2.9.4.1 Shortly following the notice of a change of address for a member account, Holy Cross receives a request for the addition of authorized users on the account.

2.9.4.2 Holy Cross is notified that the member is not receiving paper account statements, if the member is not an e-billing account.

2.9.4.3 A member requests a capital credit check or utility deposit refund check be sent to a new address.

2.9.4.4 A member requests that a capital credit check or utility deposit refund check be made payable to a person other than the member.

2.9.4.5 A member requests that Holy Cross provide the member with PII from Holy Cross's records.

MSRs shall be trained to note unusual use of accounts, or suspicious activities related to accounts and verify the identity of members in such circumstances. It shall be the policy of Holy Cross not to provide PII to members, either verbally or in writing, even when a member is asking for their own information. MSRs shall immediately notify a supervisor, who will conduct further reasonable inquiry, when a member requests their own PII. MSRs shall also notify a supervisor when there are an unusually high number of inquiries on an account, coupled with a lack of correlation in the information provided by the member.

2.9.5 Notices. Notices of potential Identity Theft are also serious Red Flags, including:

2.9.5.1 Notice from members, law enforcement authorities, or other persons indicating that a member has been a victim of Identity Theft.

2.9.5.2 Notice to Holy Cross that a member has provided PII to someone fraudulently claiming to represent Holy Cross.

2.9.5.3 Notice to Holy Cross that a fraudulent website that appears similar to Holy Cross's website is being used to solicit members' PII.

2.9.5.4 Holy Cross's mail servers are receiving returned e-mails that Holy Cross did not send indicating that a member may have received a fraudulent e-mail soliciting members' PII.

Upon notice from a member or third party, law enforcement authority or other persons that one of its members may be a victim of Identity Theft, Holy Cross shall contact the member directly to determine what steps under this Policy may be necessary to protect any member PII in possession of Holy Cross.

2.10 Preventing and Mitigating Identity Theft. If Holy Cross discovers that any of its members have become victims of Identity Theft, Holy Cross shall take appropriate steps to mitigate the impacts of such Identity Theft. These steps may include, but are not limited to:

2.10.1 Monitoring an account for evidence of Identity Theft.

2.10.2 Contacting the member.

2.10.3 Changing any passwords, security codes or other security devices that permit access to an account.

2.10.4 Placing a hold or stop payment on any outstanding capital credit refund or utility deposit refund checks.

2.10.5 Setting up a new account for the member with additional PII that may be identified only by the member to protect the integrity of the member's account.

2.10.6 Notifying the appropriate local, State or Federal authorities.

2.10.7 Determining that no response is warranted.

2.11 Policy Updates and Administration. Holy Cross shall consider updates to this Identity Theft Prevention Policy on an as needed basis to determine whether it has experienced any Identity Theft of its members' accounts, whether changes in the methods of Identity Theft require updates to this Policy, and whether changes are necessary to detect, prevent and mitigate Identity Theft.

3. RESPONSIBILITY

3.1 The Board shall be responsible for the administration of and compliance with this Policy.

3.2 The President and CEO shall ensure this Policy is adhered to by Holy Cross employees and shall serve as the Privacy Officer.