

**BANDERA ELECTRIC COOPERATIVE, INC.**

**POLICY NO. C08-2**

**ORIGINAL Sheet No. 1**

**SUBJECT: Identity Theft Prevention Program**

**EFFECTIVE: October 15, 2008**

---

---

**I. PROGRAM SUMMARY AND PURPOSE**

On November 9, 2007, the Federal Trade Commission (“FTC”) and other federal regulatory agencies published the final rule regarding Identity Theft Red Flags and Address Discrepancies (“Red Flag Rule”) pursuant to the Fair and Accurate Credit Transactions Act of 2003 (the “FACT Act”). See 16 C.F.R. Part 681. The Red Flag Rule requires utilities such as Bandera Electric Cooperative, Inc. (“BEC”) to develop and implement no later than November 1, 2008, a written Identity Theft Prevention Program that is designed to detect, prevent, and mitigate Identity Theft of consumer information in connection with a Covered Account.

Pursuant to the Red Flag Rule and the FACT Act, the Board of Directors of BEC (“Board”) adopts the following Identity Theft Prevention Program (“Program”) to: (1) identify relevant Red Flags for the covered accounts that BEC offers or maintains, and incorporate those Red Flags into this Program; (2) detect Red Flags that have been incorporated into the Program; (3) respond to any Red Flags that are detected to prevent and mitigate identity theft; and (4) ensure the Program is updated periodically, to reflect changes in risks to member-owners.

**II. DEFINITIONS**

1. “Cooperative” means Bandera Electric Cooperative, Inc.
2. “Covered account” means an account that BEC offers or maintains, primarily for personal, family or household purposes, that involves or is designed to permit multiple payments or transactions; and any other account that BEC offers or maintains for which there is a reasonably foreseeable risk to member-owner or to the safety and soundness of BEC from Identity Theft, including financial, operational, compliance, reputation, or litigation risks. Part IV identifies the types of Covered Accounts maintained by BEC that are relevant to this Program.
3. “Member-owner” means a member and owner of the Cooperative for whom the Cooperative maintains a Covered Account, an applicant applying to become a member and owner of the Cooperative by opening a Covered Account, or any other person that has a Covered Account with the Cooperative or for whom the Cooperative maintains Identifying Information.
4. “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, unique electronic identification number, address, or routing code.
5. “Identity Theft” means a fraud committed or attempted using the Identifying Information of another person without authority.
6. “Red Flag” means a pattern, practice, or specific activity that indicates the possible existence of Identity Theft. Part V provides a specific description of the Red Flags identified as relevant to the Program.
7. “Senior Management Employee” means the senior management level employee designated by the Board to implement and manage the Program.

SUBJECT: Identity Theft Prevention Program

EFFECTIVE: October 15, 2008

---

---

8. "Service Provider" means a person that provides a service directly to BEC.

**III. INCORPORATION OF EXISTING POLICIES AND PROCEDURES**

1. The following existing policies and procedures of BEC are specifically incorporated into this Program and will continue to operate in conjunction with the Program to achieve its stated purpose:
- (a) Privacy Policy No. C06-1
  - (b) Document Retention Policy No. C05-5
  - (c) Right to Access to Information and Records of the Cooperative Policy No. C04-2
  - (d) Work Rules Policy No. E04-6

**IV. IDENTIFICATION OF ACCOUNTS SUBJECT TO RED FLAG POLICY**

1. **Types of Covered Accounts.** BEC is an electric cooperative providing electric utility service to member-owners in Bandera, Bexar, Kendall, Kerr, Medina, Real and Uvalde Counties, Texas. After considering the methods it uses to open its accounts, the methods it provides to access its accounts, and its prior experience with Identity Theft, BEC has determined that it offers or maintains the following accounts that may be classified as Covered Accounts to which the Program applies:
- (a) *Payments for Electric Service Rendered.* BEC opens or maintains accounts for its member-owners that allow member-owners to pay for service after it has been rendered. Payments for service rendered are due within sixteen (16) days of billing. BEC does not regularly provide credit to its member-owners beyond this revolving, monthly account for electric service. BEC allows member-owners to pay for service rendered online through BEC's Internet website, or by automatic bank draft or recurring credit card payment. Service is delivered to a fixed physical location known to BEC. As a result, there is a low risk of misuse of Identifying Information to perpetrate fraud on the Cooperative for utility service rendered. However, Identifying Information maintained by BEC could be used to perpetrate Identity Theft and defraud other businesses if the information were wrongfully obtained, altered, or disclosed.
  - (b) *Payments for Line Extensions Security Lights, and Other Services.* BEC charges construction fees for costs of line extensions, security lighting, and other services. BEC also charges a non-refundable deposit and engineering fees for the extension of new electric service that requires construction. These services are provided to a fixed physical location known to BEC. As a result, there is a low risk of misuse of Identifying Information to perpetrate fraud on the Cooperative for these services. However, Identifying Information maintained by BEC could be used to perpetrate Identity Theft and defraud other businesses if the information were wrongfully obtained, altered, or disclosed.
  - (c) *Deposit Accounts.* For new member-owners, BEC may require deposits prior to the initiation of service. Deposit amounts are held under the terms and conditions of the membership agreement and may eventually be refunded to the member-owners. There is

**BANDERA ELECTRIC COOPERATIVE, INC.**

**POLICY NO. C08-2**

**ORIGINAL Sheet No. 3**

**SUBJECT: Identity Theft Prevention Program**

**EFFECTIVE: October 15, 2008**

---

---

some risk that a member-owner who is a victim of Identity Theft could have the member-owner's deposit refunded to an identity thief. Additionally, Identifying Information maintained by BEC could be used to perpetrate Identity Theft and defraud other businesses if the information were wrongfully obtained, altered, or disclosed.

(d) *Membership Fee Accounts.* BEC requires the payment of a membership fee upon application for membership in the Cooperative. The membership fee is held by BEC under the terms and conditions of the membership agreement and may be refunded to the member-owners. There is some risk that a member-owner who is a victim of Identity Theft could have the membership fee refunded to an identity thief. Additionally, Identifying Information maintained by BEC could be used to perpetrate Identity Theft and defraud other businesses if the information were wrongfully obtained, altered, or disclosed.

(e) *Capital Credit Accounts.* Certain member-owners are eligible for allocation of capital credits in accordance with BEC's Bylaws and Board policies. Capital credits are retired in accordance with the Bylaws and Board policies, either in the form of a check to the member-owner or a credit on the member-owner's bill. There is some risk that a member-owner who is a victim of Identity Theft could have the member-owner's capital credit retirement check sent to an identity thief. Additionally, Identifying Information maintained by BEC could be used to perpetrate Identity Theft and defraud other businesses if the information were wrongfully obtained, altered, or disclosed.

2. **Methods for Opening Accounts.** BEC uses the following methods in opening new Covered Accounts:

(a) *Information Required and Methods of Submission.* BEC requires that prospective member-owners who wish to receive electric utility service submit a membership application containing the applicant's name, signature, physical address, telephone number, social security number or tax identification number, and driver's license number or other government-issued identification number. BEC also requests that a copy of the applicant's driver's license or other government-issued identification document be submitted with the application. The application may be submitted in person, by mail, or by fax. Given the information required and the option to submit the information by mail or fax, there is a reasonably foreseeable risk of Identity Theft of member-owners' Identifying Information.

(b) *Screening Process.* Before opening a new Covered Account, BEC compares the information provided by the applicant with information contained on the applicant's government-issued identification document. BEC does not typically request a consumer report or otherwise check an applicant's credit history before opening a Covered Account.

3. **Methods for Accessing Accounts.** BEC allows member-owners to access information related to their accounts using the following methods:

(a) in person at BEC's offices with proper picture identification;

**BANDERA ELECTRIC COOPERATIVE, INC.**

**POLICY NO. C08-2**

**ORIGINAL Sheet No. 4**

**SUBJECT: Identity Theft Prevention Program**

**EFFECTIVE: October 15, 2008**

---

---

- (b) over the telephone after the member-owner provides certain Identifying Information, such as last four digits of the member-owner's social security number, the tax identification number, or driver's license number;
  - (c) by mail if the mailing contains certain Identifying Information, such as last four digits of the member-owner's social security number, the tax identification number, or driver's license number; or
  - (d) over the Internet using a unique username and secure password chosen by the member-owner.
4. **Previous Experience with Identity Theft.** To the best of its knowledge, BEC has not experienced any past incidents of Identity Theft due to a security breach of, or unauthorized access to, its systems that are used to store member-owners' Identifying Information collected by the Cooperative.

**V. IDENTIFYING RELEVANT RED FLAGS**

1. **Risk Factors.** In establishing the events and occurrences that shall be considered Red Flags for purposes of this Program, BEC examined the above Covered Accounts, including the methods by which BEC opens and grants access to the Covered Accounts and BEC's past experience with Identity Theft.
2. **Sources of Red Flags.** In incorporating relevant Red Flags into this Program, BEC has considered, and will continue to consider in its annual review of the Program, incidents of Identity Theft that BEC may experience. BEC has and will continue to consider methods of Identity Theft that reflect changes in Identity Theft risks. BEC has also considered, and will continue to consider, supervisory guidance in establishing relevant Red Flags, such as the guidelines initially published with the FTC's Red Flag Rule. In its annual review of the Program, BEC will review this and additional guidance from the FTC and other consumer protection authorities.
3. **Categories of Red Flags.** In identifying relevant Red Flags associated with the Covered Accounts that BEC maintains, BEC'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:
  - (a) *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. Such Red Flags include:
    - (i) a fraud or active duty alert is included in a consumer report;
    - (ii) a consumer reporting agency provides a notice of credit freeze in response to a request for a consumer report;
    - (iii) a consumer reporting agency provides a notice of address discrepancy; and
    - (iv) a consumer report indicates a pattern of activity that is inconsistent with the history and usual pattern of activity of an applicant or member-owner, such as:

**BANDERA ELECTRIC COOPERATIVE, INC.**

**POLICY NO. C08-2**

**ORIGINAL Sheet No. 5**

**SUBJECT: Identity Theft Prevention Program**

**EFFECTIVE: October 15, 2008**

---

---

- 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.

Required Response. Although BEC does not usually request a consumer report, if BEC receives a consumer report that indicates an information discrepancy, BEC's employees shall report any such information to a supervisor for further review and verification of the member-owner's information, which may include verifying picture identification in person at the Cooperative's offices. Employees shall look for unusual activity when reviewing a consumer report, Covered Accounts, or other member-owner information. If there is unusually high number of inquiries on a particular account, employees shall report such activity to a supervisor for further review and inquiry. The supervisor shall confer with the Senior Management Employee responsible for the Program to determine the appropriate response set out in Part VII.

- (b) *Suspicious Documents.* The presentation of suspicious documents can be a Red Flag for Identity Theft. Such Red Flags include:
  - (i) documents provided for identification appear to have been altered or forged;
  - (ii) the photograph or physical description on the identification is not consistent with the appearance of the applicant or member-owner presenting the identification;
  - (iii) other information on the identification is not consistent with information provided by the person opening a new Covered Account or member-owner presenting the identification;
  - (iv) other information on the identification is not consistent with readily accessible information that is on file with BEC, such as a membership application card; and
  - (v) an application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

Required Response. BEC's employees shall report to a supervisor when it appears that application or account documents have been altered or forged when compared to other documents in a member-owner's file. Employees shall also immediately notify a supervisor if any member-owner presents an invalid picture identification, or picture identification that appears forged, for the purpose of obtaining access to Covered Account information. The supervisor shall confer with the Senior Management

**BANDERA ELECTRIC COOPERATIVE, INC.**

**POLICY NO. C08-2**

**ORIGINAL Sheet No. 6**

**SUBJECT: Identity Theft Prevention Program**

**EFFECTIVE: October 15, 2008**

---

---

Employee responsible for the Program to determine the appropriate response set out in Part VII.

- (c) *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. Such Red Flags include:
- (i) personal Identifying Information provided is inconsistent when compared against external information sources used by BEC. For example:
    - a. the address does not match any address in the consumer report; or
    - b. the social security number has not been issued, or is listed on the Social Security Administration's Death Master File;
  - (ii) personal Identifying Information provided by the member-owner is not consistent with other personal Identifying Information provided by the member-owner. For example, there is a lack of correlation between the social security number range and date of birth;
  - (iii) personal Identifying Information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by BEC. 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;
  - (iv) personal Identifying Information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by BEC. 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;
  - (v) the social security number provided is the same as that submitted by other persons opening a Covered Account or other member-owners;
  - (vi) 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 Covered Accounts or other member-owners;

**BANDERA ELECTRIC COOPERATIVE, INC.**

**POLICY NO. C08-2**

**ORIGINAL Sheet No. 7**

**SUBJECT: Identity Theft Prevention Program**

**EFFECTIVE: October 15, 2008**

---

---

- (vii) the person opening the Covered Account or the member-owner fails to provide all required personal Identifying Information on an application or in response to notification that the application is incomplete;
- (viii) personal Identifying Information provided is not consistent with personal Identifying Information that is on file with BEC; and
- (ix) to the extent BEC uses a challenge question to confirm a member-owner's identity, the person opening the Covered Account or the member-owner cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.

Required Response. BEC shall provide member-owners access to their Covered Account information only after the member-owner has satisfied identity verification procedures. A member-owner may access Covered Account information in person at the Cooperative's offices only upon presenting appropriate picture identification that verifies the member-owner's identity. Access to Covered Account information via telephone or internet shall require the member-owner to verify his or her identity using information that would only be known to the member-owner as reflected in the member-owner's Covered Account. BEC will not disclose Identifying Information contained in an account file unless the member-owners to whom that Covered Account pertains appears in person with appropriate picture identification that verifies the member-owner's identity. Employees shall note in a member-owner's file when there is a lack of correlation between information provided by a member-owner and information contained in a file for the purposes of gaining access to Covered Account information. BEC will not provide Covered Account information without first clearing any discrepancies in the information provided. Discrepancies shall be reported to a supervisor, and the supervisor shall confer with the Senior Management Employee responsible for the Program to determine the additional responses set out in Part VII that may be required by the circumstances.

- (d) *Suspicious Activity.* The unusual use of, or other suspicious activity related to, a Covered Account is also a Red Flag for potential Identity Theft. Such Red Flags include:
  - (i) shortly following the notice of a change of address for a Covered Account, BEC receives a request for the addition of authorized users on the Covered Account;
  - (ii) mail sent to the member-owner is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the member-owner's Covered Account;
  - (iii) BEC is notified that the member-owner is not receiving paper account statements;
  - (iv) BEC is notified of unauthorized charges or transactions in connection with the member-owner's Covered Account;

**BANDERA ELECTRIC COOPERATIVE, INC.**

**POLICY NO. C08-2**

**ORIGINAL Sheet No. 8**

**SUBJECT: Identity Theft Prevention Program**

**EFFECTIVE: October 15, 2008**

---

---

- (v) a member-owner requests a capital credit or deposit refund check be sent to a new address without requesting a service disconnection or change in service location;
- (vi) a member-owner requests that a capital credit or deposit refund check be made payable to a person other than the member-owner; and
- (vii) a member-owner requests that BEC provide the member-owner with Identifying Information from the Cooperative's records.

Required Response. Employees shall note unusual use of Covered Accounts or suspicious activities related to Covered Accounts and shall verify the identity of member-owners in such circumstances. Employees shall look for unusual or suspicious activity when reviewing Covered Accounts and responding to information requests. If an employee detects unusual or suspicious activity, the employee shall immediately notify a supervisor, who will conduct further reasonable inquiry. Employees 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-owner. Supervisors made aware of suspicious activity shall confer with the Senior Management Employee responsible for the Program to determine any additional response set out in Part VII that may be required by the circumstances. It shall be the policy of BEC to not provide Identifying Information to any person, unless the member-owner to whom the Identifying Information pertains appears in person with appropriate picture identification that verifies the member-owner's identity. Depending on the circumstances, BEC may require a member-owner to appear in person with appropriate picture identification to obtain a capital credit or deposit refund check.

- (e) *Notices.* Notices of potential Identity Theft are also serious Red Flags. Such Red Flags include:
  - (i) notice from a member-owner of unauthorized charges in connection with that member-owner's Covered Account;
  - (ii) notice from member-owners, law enforcement authorities, or other persons indicating that a member-owner has been a victim of Identity Theft;
  - (iii) notice to the Cooperative that a member-owner has provided information to someone fraudulently claiming to represent the Cooperative;
  - (iv) notice to the Cooperative that a fraudulent website that appears similar to the Cooperative's website is being used to solicit member-owners' Identifying Information; and
  - (v) the Cooperative's mail servers are receiving returned e-mails that the Cooperative did not send, indicating that its member-owners may have received a fraudulent e-mail soliciting member-owners' Identifying Information.

Required Response. Upon notice that one of its member-owners may be a victim of Identity Theft, BEC shall contact the member-owner directly to determine what steps

BANDERA ELECTRIC COOPERATIVE, INC.

POLICY NO. C08-2

ORIGINAL Sheet No. 9

SUBJECT: Identity Theft Prevention Program

EFFECTIVE: October 15, 2008

---

---

may be necessary to protect the member-owner's Identifying Information in the possession of BEC. Such steps may include, but not be limited to, setting up a new Covered Account for the member-owner with additional Identifying Information that may be identified only by the member-owner to protect the integrity of the member-owner's Covered Account, notifying member-owners or law enforcement of an on-going attempt to perpetrate a fraud on the Cooperative or its membership, and complying with all applicable provisions of the Fair Credit Reporting Act. The Senior Management Employee responsible for the Program shall determine what, if any, additional steps set out in Part VII should be taken.

- (f) *Other Relevant Red Flags.* There are additional activities that may be Red Flags for Identity Theft relevant to this Program, including:
- (i) the name of an employee of BEC has been added as an authorized user on a Covered Account;
  - (ii) an employee has accessed or downloaded an unusually large number of member-owner account records;
  - (iii) BEC detects attempts to access a member-owner's Covered Account by unauthorized persons; and
  - (iv) BEC detects, or is informed of, unauthorized access to a member-owner's Identifying Information.

Required Response. If BEC becomes aware of these additional Red Flag activities, BEC shall immediately investigate the employee and affected Covered Accounts. The Senior Management Employee responsible for the Program shall determine what responses set out in Part VII may be required by the circumstances. If an employee has engaged in unauthorized or illegal activity, BEC may terminate or suspend the employee, restrict the employee's access to Covered Accounts, or report the activity to law enforcement, as circumstances may warrant.

VI. **DETECTING RED FLAGS**

1. **Opening an Account.** The primary process for opening a new Covered Account is by physical delivery of an application to BEC. While this method is the safest in terms of Identity Theft, BEC also accepts applications by mail and fax. In all instances, BEC shall use the following procedures to verify the identity of a person opening a new Covered Account and to assist BEC in detecting Red Flags.
  - (a) *Required Application Information.* To ensure proper detection of Red Flags, all member-owners must provide at least the following "Application Information" before any new Covered Account will be opened, regardless of how opened:
    - (i) name and signature;
    - (ii) physical address;

**BANDERA ELECTRIC COOPERATIVE, INC.**

**POLICY NO. C08-2**

**ORIGINAL Sheet No. 10**

**SUBJECT: Identity Theft Prevention Program**

**EFFECTIVE: October 15, 2008**

---

---

- (iii) telephone number;
  - (iv) social security number (or tax identification number for businesses)
  - (v) driver's license number or other government-issued identification number;
  - (vi) copy of driver's license or other government-issued identification document.
- (b) *In-Person Application.* Whenever possible, a member-owner should present an application and the Application Information to an authorized employee at a business center. Aside from the Application Information, the amount of Identifying Information needed for the application should be kept to a minimum. This application method affords the employee the opportunity to review and verify the Identifying Information contained in the application and to match the Identifying Information to the applicant. By carefully reviewing the Application Information, the employee can screen for potential Red Flags before a Covered Account is opened. The employee shall copy both sides of identification documents and place the copies with the member-owner's file.
- (c) *Mailed or Faxed Application.* Although mailed or faxed applications are more convenient and save time and travel, the process runs a higher risk of Identity Theft and therefore shall be carefully monitored. Application Information is still necessary with a mailed or faxed application and copies of both sides of identification documents shall be directly mailed or faxed to the appropriate business center. The copied identification documents shall be compared to the mailed or faxed application to verify the accuracy of Identifying Information.
2. **Maintaining Accounts.** BEC shall authenticate the Identifying Information of member-owners, monitor transactions, and verify the validity of change of address requests for all Covered Accounts. For any holder of an existing Covered Account for which Application Information is not already on file, BEC shall contact the member-owner within a reasonable period of time after discovering the missing Application Information to obtain and verify the Application Information.
- (a) *Physical Security.* Existing Covered Accounts and the Identifying Information included within the Covered Accounts shall be properly secured. Upon receipt, original applications and accompanying Application Information are scanned into a meta-viewer and saved in BEC's account database. Hard copies of the applications are destroyed, except for copies of identification documents, which are secured in BEC's vault for future reference in verifying member-owners' identities. Any other physical files containing Identifying Information or other Covered Account information shall be similarly housed in a secure location. Physical files shall not be accessible to the public, and shall only be accessible to the account holder upon a showing of proper picture identification that verifies the account holder's identity. As additional protection, BEC's buildings are accessible only by an access card, and non-employees are not allowed outside of member-owner service areas without an escort.
- (b) *Computer Security.* BEC's account database may be subject to breach and should be protected against unwanted and unauthorized outside access. BEC maintains Covered Account information through a software program called Daffron. Access to Daffron is secured by multiple levels of passwords, depending upon the employee's security clearance to view the information. BEC is updating Daffron to make only the last four

**BANDERA ELECTRIC COOPERATIVE, INC.**

**POLICY NO. C08-2**

**ORIGINAL Sheet No. 11**

**SUBJECT: Identity Theft Prevention Program**

**EFFECTIVE: October 15, 2008**

---

---

digits of social security numbers visible to the majority of employees using the system. In addition, each computer workstation is secured by a user password. To assist with detection of Red Flags and protect Identifying Information, BEC uses security software called Secure Works for daily monitoring of unauthorized access to its computer systems. BEC also uses a firewall program to protect its network from unauthorized access through the Internet. BEC is considering additional access controls at each desktop to further protect its network from outside access.

- (c) *Closing an Account.* When a Covered Account is closed, proper steps must be taken to dispose of the records and Identifying Information. Physical files shall be shredded and a software program shall be used to “wipe” and delete all data stored in the database.
3. **Accessing an Account.** A Covered Account will be accessible only to the member-owners to which the Covered Account pertains. A member-owner may access account information in person at a business center only upon the showing of proper picture identification that matches the information in the account database. A member-owner may access account information via telephone or mail only upon verifying his or her identity using information that would only be known to the member-owner as reflected in the member-owner’s Covered Account, such as the last four digits of the member-owner’s social security number, the member-owner’s tax identification number, or the member-owner’s driver’s license number. BEC allows member-owners to access a Covered Account and pay bills online. Online access to a Covered Account is safeguarded by a unique username and password selected by the member-owner. BEC must ensure the login process is secure at all times, either through security software or a computer security company. BEC shall monitor access to Covered Accounts and report and respond to unusual or suspicious activity. BEC will not disclose Identifying Information contained in a Covered Account file unless the member-owner to whom that Covered Account pertains appears in person with proper picture identification that verifies the member-owner’s identity.

**VII. PREVENTING AND MITIGATING IDENTIFY THEFT**

1. **Response to Red Flag Detection.** BEC is committed to preventing Identity Theft. If BEC detects a Red Flag, BEC will take the appropriate steps to prevent and mitigate any harm that could be caused by the Red Flag. In responding to a Red Flag, BEC shall consider aggravating circumstance(s) that may heighten the risk of Identity Theft. After assessing the risk posed, BEC will respond to the Red Flag in an appropriate manner, which may include:
- (a) monitoring a Covered Account for evidence of Identity Theft;
  - (b) contacting or notifying the member-owners;
  - (c) requiring the member-owners to appear in person with appropriate identification;
  - (d) changing any passwords, security codes, or other security devices that permit access to a Covered Account;
  - (e) reopening a Covered Account with a new account number;
  - (f) not opening a new Covered Account;
  - (g) closing an existing Covered Account;

**BANDERA ELECTRIC COOPERATIVE, INC.**

**POLICY NO. C08-2**

**ORIGINAL Sheet No. 12**

**SUBJECT: Identity Theft Prevention Program**

**EFFECTIVE: October 15, 2008**

---

---

- (h) not attempting to collect on a Covered Account or not selling a Covered Account to a debt collector;
  - (i) notifying law enforcement;
  - (j) putting a stop payment on any outstanding capital credit or deposit refund checks;
  - (k) putting a hold on any new capital credit or deposit refund checks; or
  - (l) determining that no response is warranted under the particular circumstances.
2. **Service Providers.** BEC may have business relationships with Service Providers who may have access to member-owners' Identifying Information. For the protection of member-owners, BEC shall ensure that the Service Provider's work for the Cooperative is consistent with this Program by (a) entering a contract with the Service Provider that incorporates the Program's requirements; (b) amending a contract with the Service Provider to incorporate these requirements; (c) if a contract cannot be amended, providing notice of the Cooperative's Program to the Service Provider and request that the Service Provider comply with the Program; or (d) otherwise determine that the Service Provider has reasonable alternative safeguards that meet or exceed the level of protection provided by this Program. BEC has identified the following Service Providers who may have access to member-owners' Identifying Information:
- (a) BEC uses banks to process member-owners' automatic bank drafts;
  - (b) BEC uses credit card service providers as a gateway to process member-owners' recurring credit card payments;
  - (c) BEC uses a collection agency to collect on bills that remain outstanding after a member-owner's electric service has been disconnected; and
  - (d) BEC uses a bill processing organization to print monthly billing statements sent to member-owners.
  - (e) BEC uses consulting engineering services to do studies, design and staking;
  - (f) BEC uses consulting services for computer, studies and IT support;
  - (g) BEC uses construction contractors to build and repair overhead and underground distribution systems;
  - (h) BEC uses ROW contractors to clear old and new rights-of-way;
  - (i) BEC uses a material warehouse operator to manage the warehouse;
  - (j) BEC uses mapping, GIS, and pole inspection contractors to do field evaluations and audits;
  - (k) BEC uses records and refuse disposal companies for documents that may contain personal identifying information;

**BANDERA ELECTRIC COOPERATIVE, INC.**

**POLICY NO. C08-2**

**ORIGINAL Sheet No. 13**

**SUBJECT: Identity Theft Prevention Program**

**EFFECTIVE: October 15, 2008**

---

- (l) BEC reports to federal and state government agencies with information as required by various laws;
  - (m) BEC uses legal services for consulting and legal advice/representation;
  - (n) BEC uses custodial services to clean buildings;
  - (o) BEC provides information to state and national organizations (TEC and NRECA), and affiliated organizations for retirement, insurance, professional and training services, and;
  - (p) BEC uses accounting and auditing services for financial consulting and audits.
3. **Opening, Maintaining, and Accessing a Covered Account.** The procedures for opening, maintaining, and accessing a Covered Account discussed in Part VI will also serve to prevent and mitigate Identity Theft.
4. **Email Confidentiality.** Any e-mails sent by BEC to member-owners shall include the following Confidentiality Statement to prevent possible Identity Theft if the e-mail is intercepted or sent to the wrong party:
- Confidentiality Statement:* The information contained in this E-mail is legally privileged and confidential information which is intended only for the use of the individual or entity to whom it is addressed. If the reader of this message is not the intended recipient, you are hereby notified that any use, dissemination, distribution or reproduction of this message is strictly prohibited. If you have received this communication in error, please notify us immediately by telephone and delete the misdirected message from your system. Thank you for your cooperation.
5. **Employees.** BEC will identify those employees that will or may have access to Identifying Information or other sensitive information. BEC may require employees or potential employees to submit to a background check to determine if they have ever been involved with or participated in any acts of fraud or Identity Theft. All employees with potential access to Identifying Information shall be trained and updated on the current privacy policies, procedures, and security measures implemented by this Program. An employee that does not handle Covered Accounts or need Covered Account information to carry out his/her daily duties should not have access to Identifying Information or other Covered Account information. Improper use of Identifying Information will subject the employee to disciplinary action and, if warranted, termination. All former employees shall be removed from access to Identifying Information and/or Covered Accounts immediately.

**VIII. PROGRAM UPDATES AND ADMINISTRATION**

1. **Updates.** BEC is committed to maintaining an Identity Theft Prevention Program that is current with the ever-changing crime of Identity Theft. To that end, BEC shall reassess this Program on at least an annual basis to determine whether changes are necessary to reflect changes in risks to member-owners or to the safety and soundness of BEC or member-owners from Identity Theft. In reassessing the Program, BEC shall consider:

**BANDERA ELECTRIC COOPERATIVE, INC.**

**POLICY NO. C08-2**

**ORIGINAL Sheet No. 14**

**SUBJECT: Identity Theft Prevention Program**

**EFFECTIVE: October 15, 2008**

---

---

- (a) BEC'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 offered or maintained by BEC; and
- (e) changes in BEC's business arrangements, including mergers, acquisitions, alliances, joint ventures, and Service Provider arrangements.

2. **Administration.** Administration of this Program shall be as follows:

- (a) *Board of Directors and Senior Management Employee.* The Board has adopted this Program and will have ultimate authority over the Program, but the Program shall be managed by the Senior Management Employee designated by the Board in Part X, or in any subsequent resolution of the Board. The Senior Management Employee shall have authority to delegate oversight and compliance to other senior management level employees. The Senior Management Employee shall be responsible for training and reviewing staff and for preparing reports regarding compliance with the Program.
- (b) *Reports and Records.* The Senior Management Employee, with the assistance of any senior management personnel assigned responsibility for this Program, shall prepare a report, at least annually, regarding the implementation, progress of, and proposed changes to the Program, if any. The Senior Management Employee shall present the report to the Board for review at least annually. The report shall address material matters related to the Program and evaluate issues such as: 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; Service Provider arrangements; significant incidents involving Identity Theft and management's response; and recommendations for material changes to the Program. The Senior Management Employee shall periodically hold meetings with other senior management level employees involved in the Program to review the progress of and proposed changes to the Program, and must hold such meetings after an Identity Theft incident. The Senior Management Employee shall keep records of meetings regarding this Program showing the dates and topics discussed. The Senior Management Employee shall maintain a file with copies of past reports prepared under the Program.
- (c) *Changes to Program.* Material changes to the Program must be approved by the Board. Meeting minutes shall contain details of the actions taken by the Board during its review process. If the Senior Management Employee determines that changes to the Program are needed prior to the meeting at which the Program is to be reviewed by the Board, the Senior Management Employee shall request an earlier meeting of the Board for that purpose.

**IX. ADDRESS DISCREPANCY REQUIREMENTS**

- 1. **Address Discrepancies.** Because BEC may sometimes use consumer reports, at least one of the following steps must be taken when BEC receives notice from any consumer reporting agency that

**BANDERA ELECTRIC COOPERATIVE, INC.**

**POLICY NO. C08-2**

**ORIGINAL Sheet No. 15**

**SUBJECT: Identity Theft Prevention Program**

**EFFECTIVE: October 15, 2008**

---

---

a substantial difference exists between the address for the member-owner that BEC has been provided and the address(es) in the consumer reporting agency's file for that particular member-owner:

- (a) compare the differing address with BEC's file in one of the following ways:
  - (i) confirm that the address information provided to BEC is the same information BEC obtains and uses to verify the member-owner's identity in accordance with the requirements of the Customer Information Program (CIP) rules located at 31 C.F.R. 103.121;
  - (ii) compare the differing address with BEC's records and files, including applications, change of address notifications, other member-owner account records, or retained CIP documentation;
  - (iii) compare the differing address with information BEC may have received from a third-party source; or
- (b) verify the information in the consumer report provided by the consumer reporting agency with the member-owner.

2. **Address Confirmation.** To ensure that BEC maintains and furnishes to a consumer reporting agency accurate address information for its member-owners, at least one of the following steps must be taken prior to providing service:

- (a) verify the address with the member-owner about whom BEC has requested a report;
- (b) review its own records to verify the address of the member-owner;
- (c) compare the address with information received from a third-party source; or
- (d) verify by other means that are reasonably available at the time.

3. **Other Requirements Relating to Consumer Reports.** BEC will comply with the following federal requirements to the extent they apply to BEC in its use of consumer reports:

- (a) pursuant to 15 U.S.C. § 1681m(f), BEC will not sell, transfer for consideration, or place for collection a debt after BEC has been notified under 15 U.S.C. § 1681c-2 that the debt has resulted from Identity Theft; and
- (b) pursuant to 15 U.S.C. § 1681m(a) and (b), BEC will notify a member-owner or employee or prospective employee of any adverse action taken by BEC as a result of information contained in a consumer report.

**X. PROVISIONS FOR ENFORCEMENT**

1. The Finance & Administration Manager is designated as the Senior Management Employee responsible for managing the Program.

**BANDERA ELECTRIC COOPERATIVE, INC.**

**POLICY NO. C08-2**

**ORIGINAL Sheet No. 16**

**SUBJECT: Identity Theft Prevention Program**

**EFFECTIVE: October 15, 2008**

---

---

2. The CEO/General Manager shall be responsible for the overall enforcement of the Program.
3. Supervisors and department heads shall enforce the Program on a day-to-day basis.