




Shelby Energy Cooperative

® A Touchstone Energy Cooperative 

RECEIVED

JUN 10 2016

PUBLIC SERVICE
COMMISSION

June 10, 2016

Mr. Aaron D. Greenwell
Acting Executive Director
Kentucky Public Service Commission
211 Sower Blvd
P O Box 615
Frankfort, KY 40602-0615

RE: Case No. 2012-00428
Response to Order Dated April 13, 2016

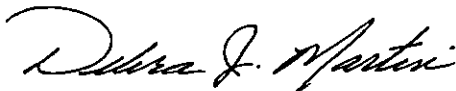
Dear Mr. Greenwell:

Enclosed are an original and three (3) copies of Shelby Energy Cooperative Inc.'s ("Shelby Energy") response to the filings required for items #4, #5 and #10, of the order.

Regarding the reference to presentations on cybersecurity procedures for each utility, Shelby Energy will work to accommodate these presentations as scheduled by the Commission.

Should you have any questions or need further information, please let us know.

Sincerely,



Debra J. Martin
President and CEO

Enclosures

www.shelbyenergy.com

620 Old Finchville Road • Shelbyville, Kentucky 40065-1714
1-800-292-6585 • Shelby Co. (502) 633-4420 • Trimble Co. (502) 255-3001 • Fax: (502) 633-2387

This institution is an equal opportunity provider and employer.

COMMONWEALTH OF KENTUCKY
BEFORE THE PUBLIC SERVICE COMMISSION

In the Matter of:

CONSIDERATION OF THE IMPLEMENTATION OF)	CASE NO.
SMART GRID AND SMART METER TECHNOLOGIES)	2012-00428

SHELBY ENERGY COOPERATIVE, INC.'S
RESPONSE TO THE COMMISSION 'S ORDER
DATED APRIL 13, 2016

SHELBY ENERGY COOPERATIVE, INC.'S
RESPONSE TO THE COMMISSION'S ORDER DATED APRIL 13, 2016
CASE NO. 2012-00428

ITEM:

4. Within 60 days of the date of this Order, the joint Utilities shall file with the Commission their internal procedures governing customer privacy and customer education.

RESPONSE:

- A. **Customer Privacy:** Refer to **Exhibit A**, pages 1-8, for a copy of Shelby Energy Cooperative Inc.'s ("Shelby Energy") Identity Theft Prevention Program Policy No. 930. In coordination with the Identity Theft Prevention Program policy, Shelby Energy has developed a Member Privacy policy which will be presented for approval at the board of directors meeting scheduled for July 15, 2016. Upon approval by Shelby Energy's board of directors, a copy of the Member Privacy policy will be submitted to the Commission.
- B. **Customer Education:** Shelby Energy has developed a Member Education and Communication policy which will be presented for approval at the board of directors meeting scheduled for July 15, 2016. Upon approval by Shelby Energy's board of directors, a copy of the Member Education and Communication policy will be submitted to the commission.

Witness: Debra J. Martin

SHELBY ENERGY COOPERATIVE, INC.'S
RESPONSE TO THE COMMISSION'S ORDER DATED APRIL 13, 2016
CASE NO. 2012-00428

ITEM:

5. Within 60 days of the date of this Order, the Joint Utilities shall certify to the Commission that they have developed internal cybersecurity procedures.

RESPONSE:

Refer to **Exhibit B** for a copy of the certification that Shelby Energy has developed internal cybersecurity procedures.

Witness: Nick Morris

SHELBY ENERGY COOPERATIVE, INC.'S
RESPONSE TO THE COMMISSION'S ORDER DATED APRIL 13, 2016
CASE NO. 2012-00428

ITEM:

10. Within 60 days of the date of this Order, the jurisdictional electric utilities shall file with the Commission their internal procedures regarding Smart Grid investments.

RESPONSE:

Refer to **Exhibit C** for a copy of Shelby Energy's Smart Grid Investments Plan.

Witness: Nick Morris

SHELBY ENERGY COOPERATIVE
Shelbyville, Kentucky

POLICY NO. 930

IDENTITY THEFT PREVENTION PROGRAM

I. OBJECTIVES

- A. To protect Shelby Energy Cooperative's ("Shelby Energy") members and their accounts from identity theft of consumer information.
- B. To comply with the requirements of the FTC and the "Red Flags" Rule.
- C. To develop and implement a written Identity Theft Prevention Program ("ITPP"), which is appropriate to our size and complexity, as well as the nature and scope of our activities.
- D. Shelby Energy's identity theft policies, procedures and internal controls, will be reviewed and updated periodically to ensure recognition of changes both in regulations and in our business.
- E. The ITPP addresses the following:
 - 1. identifying relevant identity theft Red Flags for Shelby Energy;
 - 2. detecting those Red Flags;
 - 3. responding appropriately to any Red Flags that are detected in order to prevent and mitigate identity theft and
 - 4. updating the ITPP periodically to reflect changes in regulations and Shelby Energy's business.

II. CONTENT

A. Approval and Administration

The Shelby Energy Board of Directors approved the initial ITPP and will approve future revisions to the program. The President and CEO is responsible for the overall development of the ITPP.

B. Relationship to Other Shelby Energy Programs

The Board Policies, procedures, and plans required by regulations regarding the protection of member information, including policies and procedures regarding data safekeeping and red flag detection have been reviewed. Those documents were modified or this ITPP has been created or revised to minimize inconsistencies and duplicate efforts.

C. Identifying Relevant Red Flags

To identify relevant identity theft Red Flags, Shelby Energy assessed the following risk factors:

1. the types of covered accounts it offers;
2. the methods it provides to open or access these accounts and
3. previous experience with identity theft.

Shelby Energy also considered the sources of Red Flags, including any prior identity theft incidents experienced, changing identity theft techniques that Shelby Energy thinks may be likely and applicable supervisory guidance.

In addition, Shelby Energy considered Red Flags from the following five categories:

1. alerts, notifications or warnings from a credit reporting agency;
2. suspicious documents;
3. suspicious personal identifying information;
4. suspicious account activity and
5. notices from other sources.

Shelby Energy understands that some of these categories and examples may not be relevant and some may be relevant only when combined or considered with other indicators of identity theft. Shelby Energy also understands that the examples are not exhaustive or a mandatory checklist, but a way to help Shelby Energy think through relevant red flags in the context of our business.

Based on this review of the risk factors, sources, and FTC examples of red flags, we have identified Shelby Energy's Red Flags, which are contained in the first column ("Red Flag") of the attached "Red Flag Identification and Detection Grid" ("Grid").

D. Detecting Red Flags

Shelby Energy has reviewed applicable accounts, how these accounts are opened and maintained, and how to detect Red Flags that may occur. Detection of those Red Flags is based on Shelby Energy's methods of obtaining information about members, authenticating those who access the accounts, monitoring various transactions and validating change of address requests.

Based on this review, Shelby Energy has included in the second column ("Detecting the Red Flag") of the attached Grid how to detect each of Shelby Energy's identified Red Flags.

E. Preventing and Mitigating Identity Theft

Shelby Energy has reviewed the applicable accounts, how we open and allow access to the accounts, and our previous experience with identity theft, as well as new methods of identity theft we have seen or foresee as likely.

Based on this and review of the FTC's identity theft rules and its suggested responses to mitigate identity theft, as well as other sources, we have developed the procedures below to respond to detected identity theft Red Flags.

When Shelby Energy has been notified of a Red Flag or established detection procedures show evidence of a Red Flag, Shelby Energy will take the steps outlined below, as appropriate to the type and seriousness of the threat regarding applicants and the Red Flags raised by someone applying for an account:

Procedures to Prevent and Mitigate Identity Theft

1. Review the member application.
Shelby Energy will review the applicant's information collected; name, date of birth, address, and an identification number such as a Social Security Number or Taxpayer Identification Number.
2. Independent verification.
Shelby Energy will perform verification of the applicant's information by comparing it with information from a credit reporting agency.
3. Get government identification.
If any of the above information indicates invalid data, then the applicant must apply in person. Shelby will check two current government-issued identification cards, such as a US passport, state-issued driver's license or state/federal-issued identification card,
4. Potential Risk.
If the potential risk of identity theft indicated by the Red Flag is probable or large in impact, we may also verify the person's identity through non-documentary methods, including:
 - a. contacting the customer;
 - b. checking references with other affiliated financial institutions, or
 - c. obtaining a financial statement.
5. Deny the member application.
If Shelby Energy finds that the applicant is using an identity other than his or her own, service will be denied for the account.
6. Report.
If Shelby Energy finds that the applicant is using an identity other than his or her own, it will be reported to the appropriate local and state law enforcement; where organized or wide spread crime is suspected, the FBI or Secret Service; and if mail is involved, the US Postal Inspector. The information may also be reported to the Securities and Exchange Commission and State regulatory authorities.

7. Notification.

If Shelby Energy determines personally identifiable information has been accessed that results in a foreseeable risk for identity theft, Shelby Energy will prepare a specific notice to the member(s) or other notification required under state law.

8. Access seekers.

For Red Flags raised by someone seeking to access an existing member's account, the following steps will be taken:

a. Watch.

Shelby Energy will monitor, limit, or temporarily suspend activity in the account until the situation is resolved.

b. Check with the member.

Shelby Energy will contact the member using current information on record, describe what has been discovered and verify that there has been an attempt at identify theft.

c. Heightened risk.

Shelby Energy will determine if there is a particular reason that makes it easier for an intruder to seek access, such as a member's lost wallet, mail theft, a data security incident, or the member's giving account information to an imposter pretending to represent Shelby Energy or to a fraudulent web site.

d. Check similar or related accounts.

Shelby Energy will review similar or related accounts to verify if there has been unauthorized attempts to access the accounts.

e. Report.

If unauthorized account access is determined, Shelby Energy will report it to appropriate local and state law enforcement; where organized or wide spread crime is suspected, the FBI or Secret Service; and if mail is involved, the US Postal Inspector.

f. Notification.

If Shelby Energy determines personally identifiable information has been accessed that results in a foreseeable risk for identity theft, Shelby Energy will prepare a specific notice to the member(s) or other notification required under state law.

g. Review of insurance policy.

Since insurance policies may require timely notice or prior consent for any settlement, Shelby Energy will review its current insurance policy to ensure that a response to a data breach does not limit or eliminate Shelby Energy's insurance coverage.

h. Assist the member.

Shelby Energy will work with members to minimize the impact of identity theft by taking the following actions, as applicable:

- i. offering to change the password, security code or other ways to access the threatened account;
- ii. offering to close the account;
- iii. offering to reopen the account with a new account number;

- iv. not collecting on the account or selling it to a debt collector;
and
- v. instructing the customer to go to the FTC Identity Theft Web Site to learn what steps to take to recover from identity theft, including filing a complaint using its online complaint form, calling the FTC's Identity Theft Hotline 1-877-ID-THEFT (438-4338), TTY 1-866-653-4261, or writing to Identity Theft Clearinghouse, FTC, 6000 Pennsylvania Avenue, NW, Washington, DC 20580.

F. Internal Compliance Reporting

Shelby Energy management and support staff, who are responsible for developing, implementing and administering the ITPP, will report at least annually to the Board of Directors on compliance with the FTC's Red Flags Rule. The report will address the effectiveness of the ITPP in addressing the risk of identity theft in connection with covered account openings, existing accounts, service provider arrangements, significant incidents involving identity theft and management's response and recommendations for material changes to the ITPP.

G. Updates and Review

Shelby Energy will update the ITPP whenever there is a material change to the operations, structure, business or location or when Shelby Energy experiences either a material identity theft from a covered account, or a series of related material identity thefts from one or more covered accounts. Shelby Energy will also follow new ways that identities can be compromised and evaluate the risk posed for Shelby Energy and its members.

III. RESPONSIBILITY

Each departmental Vice President, Manager and information technology staff, in direct cooperation with the President and CEO, are responsible for the administration of this policy.

Adopted: April 23, 2009
Revised: March 18, 2010
April 17, 2014

ATTACHMENT: APPENDIX I - Red Flag Identification and Detection Grid (Grid)

APPENDIX I
Red Flag Identification and Detection Grid

Red Flag	Detecting the Red Flag
Category: Alerts, Notifications or Warnings from a Consumer Credit Reporting Agency	
1. A fraud or active duty alert is included on a consumer credit report.	Verify that the fraud or active duty alert covers an applicant /member and review the allegations in the alert
2. A notice of credit freeze is given in response to a request for a consumer credit report.	Verify that the credit freeze covers an applicant/member and review the freeze.
3. A notice of address or other discrepancy is provided by a consumer credit reporting agency.	Verify that the notice of address or other discrepancy covers an applicant/member and review the address discrepancy. Shelby Energy will use internal records and other available resources to investigate the discrepancy.
4. A consumer credit report shows a pattern inconsistent with the person's history, such as a big increase in the volume of inquiries or use of credit, especially on new accounts; an unusual number of recently established credit relationships; or an account closed because of an abuse of account privileges.	Verify that the consumer credit report covers an applicant/member, and review the degree of inconsistency with prior history.
Category: Suspicious Documents	
5. Identification presented looks altered or forged.	Employees and their supervisors, who deal with applicants/members, will scrutinize identification presented in person to verify the identification is not altered or forged.
6. The person presenting the identification does not look like the identification's photograph or physical description.	Employees and their supervisors, who deal with applicants/members, will ensure that the photograph and the physical description on the identification match the person presenting it.
7. Information on the identification differs from what the person presenting the identification is stating.	Employees and their supervisors, who deal with applicants/members, will ensure that the identification and the statements of the person presenting it are consistent.
8. Information on the identification does not match other information Shelby Energy has on file for the person presenting the identification, such as the original account application, signature card or a recent check.	Employees and their supervisors, who deal with applicants/members, will ensure that the identification presented and other information we have on file from the account, are consistent.

<p>9. The application looks like it has been altered, forged or torn up and reassembled.</p>	<p>Employees and their supervisors, who deal with applicants/members, will scrutinize each application to make sure it is not altered, forged, or torn up and reassembled.</p>
<p>Category: Suspicious Personal Identifying Information</p>	
<p>10. Inconsistencies exist between the information presented and other things we know about the person presenting the data or can find out by checking readily available external sources, such as an address that does not match a consumer credit report, or the Social Security Number (SSN) has not been issued or is listed on the Social Security Administration's (SSA's) Death Master File.</p>	<p>Employees will check personal identifying information presented to Shelby Energy to ensure that the SSN given has been issued but is not listed on the SSA's Master Death File. If a consumer credit report is processed, Shelby Energy will verify the addresses on the application and the consumer report match.</p>
<p>11. Inconsistencies exist in the information provided to Shelby Energy, such as a date of birth that does not fall within the number range on the SSA's issuance tables.</p>	<p>Employees will check personal identifying information presented to verify it is internally consistent by comparing the date of birth to confirm it falls within the number range on the SSA's issuance tables.</p>
<p>12. Personal identifying information presented has been used on an account Shelby Energy knows was fraudulent.</p>	<p>Employees will compare the information presented with addresses and phone numbers on accounts or applications found to be or were reported as fraudulent.</p>
<p>13. Personal identifying information presented suggests fraud, such as an address that is fictitious, a mail drop, or a prison; or a phone number is invalid, or represents a pager or answering service.</p>	<p>Employees will validate the information presented when opening an account by looking up addresses on the Internet to ensure they are real and not for a mail drop or a prison, and will call the phone numbers given to ensure they are valid and not for pagers or answering services.</p>
<p>14. The SSN presented was used by someone else opening an account or other customers.</p>	<p>Employees will compare the SSNs presented to see if they were given by others opening accounts or other customers.</p>
<p>15. The address or telephone number presented has been used by many other people opening accounts or other customers.</p>	<p>Employees will compare address and telephone number information to see if they were used by other applicants and customers.</p>
<p>16. A person who omits required information on an application or other form and does not provide it when told it is incomplete.</p>	<p>Employees will track when applicants or customers have not responded to requests for required information and will follow up with the applicants or customers to determine why they have not responded.</p>
<p>17. Inconsistencies exist between what is presented and what Shelby Energy Cooperative has on file.</p>	<p>Employees will verify key items from the data presented with the information on file.</p>

<p>18. A person making an account application or seeking access cannot provide authenticating information beyond what would be found in a wallet or consumer credit report, or cannot answer a challenge question.</p>	<p>Employees will authenticate identities for existing customers by asking challenge questions that have been prearranged with the customer and for applicants or customers by asking questions that require information beyond what is readily available from a wallet or a consumer credit report.</p>
<p>Category: Suspicious Account Activity</p>	
<p>19. Soon after Shelby Energy receives a change of address request for an account, we are asked to add additional access means (such as debit cards or checks) or authorized users for the account.</p>	<p>Verify change of address requests by sending a notice of the change to both the new and old addresses so the customer will learn of any unauthorized changes and can notify us.</p>
<p>20. A new account exhibits fraud patterns, such as where a first payment is not made or only the first payment is made, or the use of credit for cash advances and securities easily converted into cash.</p>	<p>Review a new account activity to ensure that first and subsequent payments are made, and that credit is primarily used for other than cash advances and securities easily converted into cash.</p>
<p>21. An account develops new patterns of activity, such as nonpayment inconsistent with prior history.</p>	<p>Review our accounts on at least a monthly basis and check for suspicious new patterns of activity such as nonpayment.</p>
<p>22. An account that is inactive for a long time is suddenly used again.</p>	<p>Review our accounts on at least a monthly basis to see if long inactive accounts become very active.</p>
<p>23. Mail Shelby Energy sends to a customer is returned repeatedly as undeliverable even though the account remains active.</p>	<p>Note any returned mail for an account and immediately check the account's activity.</p>
<p>24. Discover that a customer is not getting his or her paper account statements.</p>	<p>Record on the account any report that the customer is not receiving paper statements and immediately investigate them.</p>
<p>25. Notified that there are unauthorized charges or transactions to the account.</p>	<p>Verify if the notification is legitimate and involves a Shelby Energy account, and then investigate the report.</p>
<p>Category: Notice From Other Sources</p>	
<p>26. Informed that an account has been opened or used fraudulently by a customer, an identity theft victim, or law enforcement.</p>	<p>Verify that the notification is legitimate and involves a Shelby Energy account, and then investigate the report.</p>
<p>27. Informed that unauthorized access to the customer's personal information took place or became likely due to data loss (e.g., loss of wallet, birth certificate, or laptop), leakage, or breach.</p>	<p>Contact the customer to learn the details of the unauthorized access to determine if other steps are warranted.</p>

CERTIFICATION

Pursuant to the Kentucky Public Service Commission's Order dated April 13, 2016 in Case No. 2012-00428, the undersigned, Nick Morris, states that he is Manager of Engineering for Shelby Energy Cooperative, Inc. ("Shelby Energy") and hereby certifies that Shelby Energy has developed basic policies and procedures addressing internal cybersecurity.

Shelby Energy has partnered with Jackson Technologies, LLC, an independent IT consultant that specializes in information technology security and services, to further enhance current policies and procedures. Jackson Technologies staff hold the following certifications: CISA (Certified Information Systems Auditor), MCITPEA (Microsoft Certified IT Professional – Enterprise Administrator), MCSE (Microsoft Certified Systems Engineer), CCNA (Cisco Certified Network Associate). Shelby Energy's policies will be enhanced in coordination with the results of the *Cyber Security Risk Assessment & Risk Mitigation Plan Review for the Kentucky Public Service Commission* as performed by C.H. Guernsey & Company and the *Cybersecurity Policy Framework* as developed by the KAEC IT Association.

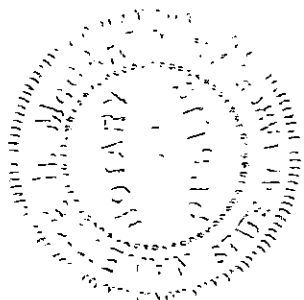
Dated: 06-02-16

By: Nick Morris
Nick Morris, Manager of Engineering

STATE OF KENTUCKY
COUNTY OF SHELBY

Subscribed, sworn to, and acknowledged before me by Nick Morris as Manager of Engineering for Shelby Energy Cooperative, Inc. this 2nd day of June, 2016.

Nanette H. McCasky ID#555678
Notary Public, Kentucky State at Large



My commission expires: 4/25/20

Smart Grid Investments

I. System Description

Shelby Energy Cooperative, Inc. ("Shelby Energy") is a rural electric cooperative headquartered at 620 Old Finchville Road in Shelbyville, KY. We serve industry, schools, farms, homes, and businesses in one of the fastest growing areas of the state. We have approximately 15,900 meters located in our service territory which includes the following counties in Kentucky: Anderson, Carroll, Franklin, Henry, Jefferson, Oldham, Owen, Shelby, Spencer, and Trimble. We have annual sales in excess of \$45 million and more than \$67 million in physical plant and facilities.

To date, we have successfully implemented an Advanced Metering Infrastructure (AMI) system which afforded us the ability to improve our System Operations, Safety for Members and Public, Member Services, Accounting & Finances, and Member Satisfaction. Such improvements include: implementation of Meter Data Management System (MDMS), reduction in the time for meter reads, increased meter reading accuracy, improved billing accuracy, easier energy theft detection, improved outage management, safer working environment for field employees via remote connect/disconnect capabilities, faster service restoration, and provided the ability to offer a Prepay Service to our members.

II. Planning Goals

Investments in Smart Grid Components must be consistent with our mission to provide safe, reliable, and cost-effective energy service.

As new technologies become available, we will evaluate the benefits and impact that each will have on our business operations and our members prior to making a decision to implement.

At the time of this writing, Shelby Energy has no immediate plans for new investment in Smart Grid Components.

III. How Investments Will Be Considered

Investments in new Smart Grid Components will be evaluated for potential impacts in relation to our System Operations, Customer Service, Finances, and Safety. Evaluating Smart Grid Components on these measures directly correlate to our mission statement of providing safe, reliable, and cost-effective energy service.