



LICKING VALLEY
RURAL ELECTRIC COOPERATIVE CORPORATION
P. O. Box 605 • 271 Main Street
West Liberty, KY 41472-0605
(606) 743-3179



RECEIVED

JUN 13 2016

PUBLIC SERVICE
COMMISSION

June 10, 2016

Aaron Greenwell
Acting Executive Director
Kentucky Public Service Commission
PO Box 615
Frankfort KY 40602-0615

RE: Case No. 2016-00428
Consideration of the Implementation
of Smart Grid and Smart Meter Technologies

Dear Aaron Greenwell:

Enclosed are an original and three (3) copies of Licking Valley Rural Electric Cooperative Corporation's response to the above referenced case number. I have enclosed responses to items 4, 5 and 10.

If there are any questions or any further information needed please contact me.

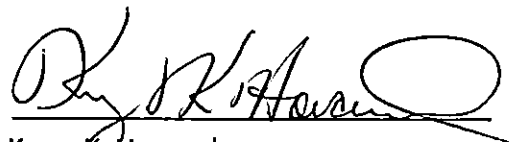
Sincerely,

Kerry K. Howard
General Manager/CEO
kkhoward@lvrecc.com
Fax – 606-743-7775



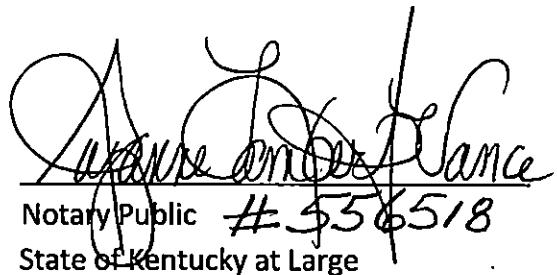
AFFIDAVIT

The Affiant, Kerry K. Howard, General Manager/CEO for Licking Valley Rural Electric Cooperative Corporation, Post Office Box 605, West Liberty, Kentucky 41472-0605, states that the answers given by him to the foregoing questions are true and correct to the best of his knowledge and belief.



Kerry K. Howard
General Manager/CEO

Subscribed and sworn before me by the Affiant, Kerry K. Howard, this 10th day of June 2016.



Notary Public #556518
State of Kentucky at Large

My Commission Expires: 05/29/2020

INDEX

Exhibit 1 – (Policy 233)” Identity Theft Prevention Program (“Red Flag”) Fact Act (Federal Register 16 CFR 681)

Exhibit 2 – (Policy 235) Privacy Policy

Exhibit 3 – Certification of Internal Cybersecurity Procedure.

LICKING VALLEY RURAL ELECTRIC COOPERATIVE CORPORATION

PSC CASE NO. 2012-00428

CONSIDERATION OF THE IMPLEMENTATION OF SMART GRID AND SMART
METER TECHNOLOGIES

Question 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: *Attached is Exhibit 1 (Policy 233) "Identity Theft Prevention Program ("Red Flag") Fact Act (Federal Register 16 CFR 681)*

Attached Exhibit 2 (Policy 235) Privacy Policy.

Customer (Member) education:

Licking Valley RECC uses local newspapers, Kentucky Living, banners, counter cards, social media (Facebook and Twitter) for member education. Licking Valley's website www.lvrecc.com contains most of the customer information and can be updated quickly. Radio and local TV are used for items for immediate release.

Instant messaging can also be used via land lines, cell phone and email accounts. This is primarily used for outage information. This means of communication is especially helpful with planned outages.

Licking Valley RECC uses NISC's online portal "Smarthub" that allows members to pay their bills on line or via an app on smartphones. This allows members to view current usage, view past bills.

Members can contact our office personnel with any questions related to our member assisted programs.

Question 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: *Attached Exhibit 3* - Licking Valley RECC certifies that we have developed an internal cybersecurity procedure; Policy Number 234

Question10. 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: Licking Valley Rural Electric Cooperative Corporation (Licking Valley RECC) is a rural electric cooperative headquartered on Highway 460 in West Liberty, Kentucky. Licking Valley RECC primarily serves four counties in Eastern Kentucky via 2,059 miles of electric distribution lines.

At the end of 2015 the number of consumers served was 17,260. The consumer base is 80% residential and 20% commercial.

Licking Valley RECC currently uses Landis + Gyr meter technology. 5 of our 10 substations are TS2 ready. We have deployed 3563 TS2 meters; 13,764 TS1 meters; and 96 RF meters.

Licking Valley RECC has filed with the PSC a CPCN application (Case Number 2016-00077).

Licking Valley RECC procedures regarding Smart Grid investments:

Assess the need for consideration of Smart Grid technology to insure that Licking Valley RECC can meet the demand and needs of its Members. If there is a need for additional application of Smart Grid technology, a cost analysis would be sought. If this analysis proves that an update with Smart Grid technology is needed, Licking Valley RECC will apply for a CPCN with the PSC. A representative from RUS would be included for loan considerations if Smart Grid technology is needed.

Executive Abstract

Board Policy 233 represents our response to the Federal Trade Commission's mandate for all American utilities to develop and implement an identity theft prevention program by November 01, 2008. This legislation is found under the Red Flag rules of the FACT Act. (Federal Register 16 CFR 681). The written plan contains:

- Privacy Committee Members and Responsibilities
- Results of a study of present vulnerability of customer secured information and strategies for improvement.
- Identity Theft Prevention Program Policies and Procedures
- Employee Education Materials
- Forms for Tracking Incidents, Analyzing Data and Report Preparation
- Program Checklist to include IT Internal and External Audits

Implementation of the Identity Theft Prevention Program requires the approval of the Board of Directors. Once approved, the first step will be to train designated employees on a need to know basis. Strategies for preventing, detecting and monitoring identity theft will be coordinated by regional and departmental management. The Board will receive an annual report to include program outcomes and goals.

LICKING VALLEY RURAL ELECTRIC COOPERATIVE CORPORATION

KENTUCKY 56 MORGAN

BOARD OF DIRECTORS POLICIES AND PROCEDURES MANUAL

Policy Number 233

Effective Date: 03/20/2014

**SUBJECT: IDENTITY THEFT PREVENTION PROGRAM ('RED FLAG')
FACT ACT (FEDERAL REGISTER 16 CFR 681)**

Page 01 of 60

Program Development by the Privacy Committee

Licking Valley Rural Electric Cooperative Corporation has developed an Identity Theft Prevention Program designed to detect, prevent and mitigate theft in connection with the opening or maintaining of any covered account.

The program is consistent with the utility's mission to provide quality service in an effective manner.

Privacy Committee

On September 25, 2008, the Privacy Committee was formed under the leadership of Kerry K. Howard, General Manager/CEO.

Representation from key areas included:

Name	Department	Responsibilities/Areas of Expertise
Suzanne Lambert Vance	Secretary to the General Manager/CEO	Privacy Officer – coordinates activities of the committee/ develop and evaluation of program. Reports to Senior Management/BOD.
Kerry K. Howard	Senior Management	Supply resources to establish the Identity Theft Program.
Sandra N. Bradley	Accounting	Personnel Information and expert in the flow of funds.
Mindy Shaver	IT Billing	Data security.
Gina Jenkins	Billing	Identity Theft Training.
Stacey Stacy	Customer Service	Opens new accounts and has the ability to monitor existing accounts.

LVRECC Board Policy Number 233

Effective Date: 03/20/2014

**SUBJECT: IDENTITY THEFT PREVENTION PROGRAM ('RED FLAG')
FACT ACT (FEDERAL REGISTER 16 CFR 681)**

Page 02 of 60

NEEDS ASSESSMENT

On September 25, 2008, Licking Valley Rural Electric Cooperative Corporation conducted a needs assessment of the flow of secured information during the processes of opening a new account as well as monitoring transactions on existing accounts. A review of red flags in the industry and the examples outlined in the FACT Act legislation served as the basis for comparing present policies and procedures against those needed to detect, prevent and mitigate identity theft. The following strengths and areas for improvement were identified:

Opening Accounts

Strengths:

Presently require all consumers to apply for service in person with photo ID and social security number.

Areas for Improvement:

Only one consumer at any time in the designated office can apply for service. Lock computers when away from your desk. Change monitors to where only the employee can see it. Shred all consumer related notes in a timely manner. Office reconstruction such as extra doors, privacy shields, etc. for more consumer privacy.

Monitoring Transactions in Existing Accounts

Strengths:

When a consumer calls in the office ask them for their account number(s) or social security number before giving out information on the account(s).

Areas for Improvement:

Consumer should to give the last 4 digits of their social security number. Use a third party to validate.

LVRECC Board Policy Number 233

Effective Date: 03/20/2014

**SUBJECT: IDENTITY THEFT PREVENTION PROGRAM ('RED FLAG')
FACT ACT (FEDERAL REGISTER 16 CFR 681)**

Page 03 of 60

CONDUCTING A NEEDS ASSESSMENT

Opening a New Account

Identify the steps in establishing electrical service for a customer.

1. What identification is required? How do you obtain identifying information and verify identity?

Drivers license, government issued photo ID, social security card, or birth certificate. Verify identification by inspecting photo, signature, and all listed information.

2. Do they need to make the application in person or can they send in the information in an alternate form? Telephone or other?

Must apply in person, no open accounts will be taken by phone.

3. Does the utility use consumer reports in the application process? How? Establish deposit? Approve or deny services?

No, not at this time.

4. Does the utility have policies and procedures that define red flags for identity theft and actions for mitigation?

(See *Taking the Right Step*)

5. What happens to the hand written notes made by the CSR in the application process?

Shred consumer related notes in a timely manner.

6. Is the computer screen visible to others during the application process?

Yes. All monitors will be positioned to where only employees can see information.

7. Who has access to data once entered? Does the CSR lock computer when not at desk?

Any/all CSR employees have access to data after information is entered. Any/all CSR employees log off computer when away from desk.

LVRECC Board Policy Number 233

Effective Date: 03/20/2014

**SUBJECT: IDENTITY THEFT PREVENTION PROGRAM ('RED FLAG')
FACT ACT (FEDERAL REGISTER 16 CFR 681)**

Page 04 of 60

8. If applicant gives address, bank account, date of birth or social security number verbally to CSR, what precautions are taken from others hearing?

Only one person is permitted in the room at a time.

9. Once personal identification information is entered by CSR, where and how can it later be retrieved:

Personal identification information can be retrieved through customer information software.

10. What safeguards are currently built into the application process?

No social security number prints on work order.

11. What safeguards would you like to implement?

Change monitor position, privacy screen filters, and changing the process work orders are taken. Not repeating personal information out loud so that other individuals can hear. Shred all consumer related notes in a timely manner. Do not permit anyone behind the cashier counter except employees.

12. Which employees have access to information – is it on a “need to know” basis?

All office personnel have access to information at any time.

13. Is any customer personal information carried into the field on a laptop?

No.

LVRECC Board Policy Number 233

Effective Date: 03/20/2014

**SUBJECT: IDENTITY THEFT PREVENTION PROGRAM ('RED FLAG')
FACT ACT (FEDERAL REGISTER 16 CFR 681)**

Page 05 of 60

Map out the steps that occur when opening a new account. Is customer identification validated? Is so, how? Trace the flow of secured information.

Customer Initial Contact

Service is Established

LVRECC Board Policy Number 233

Effective Date: 03/20/2014

**SUBJECT: IDENTITY THEFT PREVENTION PROGRAM ('RED FLAG')
FACT ACT (FEDERAL REGISTER 16 CFR 681)**

Page 06 of 60

Monitoring an Existing Account

Identify the possible red flags that may exist in the following procedures:

- Authenticating transactions for existing customers
- Monitoring activity/transaction of customers
- Verifying the validity of change of billing address
- Does the utility have policies and procedures that define red flags for identity theft and action for mitigation for existing accounts?

1. Does your utility use passwords or some form of security access?

No, ask consumers for their account number or social security number.

2. Describe your process for verifying validating the following:

- a. Check by phone: No
- b. Credit Card Number: N/A
- c. Are receipts ever printed? If so, what part of number is exposed?:
Yes, payment receipts, including the entire account number(s).

3. In what manner have customers attempted to fraudulently represent themselves as someone else in a transaction in an existing account?

None

4. What safeguards are currently built into monitoring existing utility accounts?

Verifying drivers license, government issued photo ID, social security card, or birth certificate. Verify identification by inspecting photo, signature, and all listed information.

5. What safeguards would you like to implement?

Continue to verify drivers license, government issued photo ID, social security card, or birth certificate. Verify identification by inspecting photo, signature, and all listed information.

LICKING VALLEY RURAL ELECTRIC COOPERATIVE CORPORATION

KENTUCKY 56 MORGAN

BOARD OF DIRECTORS POLICIES AND PROCEDURES MANUAL

Policy Number 233

Effective Date: 03/20/2014

**SUBJECT: IDENTITY THEFT PREVENTION PROGRAM ('RED FLAG')
FACT ACT (FEDERAL REGISTER 16 CFR 681)**

Page 07 of 60

PURPOSE:

The goal of this policy is to prevent identity theft. Licking Valley Rural Electric Cooperative Corporation recognizes the responsibility to safeguard personal customer information within the workplace. The purpose of this policy is to create an Identity Theft Prevention Program utilizing guides set forth in the FACT Act (2003).

SCOPE:

This policy applies to management and all personnel of Licking Valley Rural Electric Cooperative Corporation.

RESPONSIBILITY:

Licking Valley Rural Electric Cooperative Corporation must protect customer data and implement policies and procedures that meet standards established by the Federal Trade Commission by November 01, 2008.

DEFINITIONS:

IT - Information Technology

Identity Theft – Financial identity theft occurs when someone uses another consumer's personal information (name, social security number, etc.) with the intent of conducting multiple transactions to commit fraud that results in substantial harm or inconvenience to the victim. This fraudulent activity may include opening deposit accounts with counterfeit checks, establishing credit card accounts, establishing line of credit, or gaining access to the victim's accounts with the intent of depleting the balances.

Company - For the purposes of this policy, Licking Valley Rural Electric Cooperative Corporation is referred to as Company.

Red Flag – A pattern, particular specific activity that indicates the possible risk of Identity theft.

PROCEDURE:

A. Implementing the Program

1. Form an Identity Theft Prevention Protection Committee

Establish an identity theft prevention committee to create drive and monitor the program. Select members from Senior Management, Accounting, IT, Human Resources and Customer Service.

LICKING VALLEY RURAL ELECTRIC COOPERATIVE CORPORATION

KENTUCKY 56 MORGAN

BOARD OF DIRECTORS POLICIES AND PROCEDURES MANUAL

Policy Number 233

Effective Date: 03/20/2014

**SUBJECT: IDENTITY THEFT PREVENTION PROGRAM ('RED FLAG')
FACT ACT (FEDERAL REGISTER 16 CFR 681)**

Page 08 of 60

2. Assign Responsibilities to Committee Members

Responsibilities should be directly related to individual members' areas of expertise.

3. Appoint a Privacy Officer

Privacy officer functions as the head of committee. He/she reports to a member of Senior Management, i.e.: General Manager/CEO regarding the outcomes and needs of the identity theft prevention program.

B. Assess Company's Need for New/Updated Policies and Procedures

The following represent the core of the procedures for the Identity Theft Prevention Program.

LVRECC Board Policy Number 233

Effective Date: 03/20/2014

**SUBJECT: IDENTITY THEFT PREVENTION PROGRAM ('RED FLAG')
FACT ACT (FEDERAL REGISTER 16 CFR 681)**

Page 09 of 60

Identity Theft Prevention Program

Policy: Licking Valley Rural Electric Cooperative Corporation complies with the FACT Act by:

Subsection Number 1

Defining Action(s) to be taken for each of the Red Flags which relate to the opening of new accounts and the monitoring of existing accounts.

Procedure:

Licking Valley Rural Electric Cooperative Corporation has developed the following procedures designed to detect, prevent and mitigate identity theft in connection with the opening of a covered account or any existing covered account.

All procedures represent a typical but not absolute response. Each situation can and will have circumstances, which will be affected by a number of variables.

Licking Valley Rural Electric Cooperative Corporation submits the following managerial responses as typical but not limited to:

Flag	Next Step	Mitigation (Steps to Control Losses)
Consumer report indicates fraud or active duty alert.	Verify the information is entered correctly.	Document name/ date and what they were trying to do.
Credit freeze.	Ask them to take it off.	
Notice of address discrepancy.	Provide an address restriction on policy.	
Unusual patterns in activity.	N/A	N/A

Flag	Next Step	Mitigation (Steps to Control Losses)
Identification documents appear altered or forged.	Hold service until proper ID can be shown and validated.	Document
Photo/physical description does not match applicant.	Hold service until proper ID can be shown and validated.	Consumer – get updated.
Other information on identification is inconsistent information given from applicant.	Hold service until proper ID can be shown and validated.	Consumer – get updated.
Information in utility files in inconsistent with information provided. Example – signatures do not match on signature card.	Hold service until proper ID can be shown and validated.	Consumer – get updated.
Application looks altered or forged or destroyed and reassembled.	N/A	N/A
Identification is inconsistent with external source such as:		
<ul style="list-style-type: none"> - Address v. Address on Consumer Report - Social security number not issued. - Social security number on Death Master File. - Inconsistent information, such as lack of correlation between date of birth and social security number. 	<p>N/A</p> <p>Put on hold.</p> <p>Put on hold.</p> <p>Check if parent and child have same name and if parent has passed away recently.</p> <p>Otherwise not right.</p>	

Flag	Next Step	Mitigation (Steps to Control Losses)
<p>Identification is known to be associated with fraudulent activity:</p> <ul style="list-style-type: none"> - The address is fictitious, a prison or a mail drop on application. - The phone number is invalid or associated with a pager or answering service. - The social security number is the same as that submitted by other persons opening an account. - The address is the same address as that submitted by other persons opening an account. 	<p>N/A</p> <p>N/A</p> <p>Note: How will you distinguish customers who own rental property, barns, etc. and have multiple accounts under the same information?</p> <p>N/A</p>	<p>If all possible, accounts note if barn, trailer, house, etc.</p>
Applicant fails to provide all personal ID requested.	Hold service order until proper ID can be shown and validated.	
Personal ID is inconsistent with utility records.	Investigate, hold service order until proper ID can be shown and validated.	
For institutions using challenge questions, the person attempting to access or open the account can not provide any information beyond what would typically be found in a wallet or consumer report.	Hold service if they can't answer the question. Tell them to come in.	
Change of billing address is followed by request for adding additional properties to the account (or shortly following the notification of a change in address, the utility receives a request for the addition of authorized users on the account).	Follow-up, investigate to be assured valid.	

Flag	Next Step	Mitigation (Steps to Control Losses)
Payments are made in a manner associates with fraud. For example, deposit or initial payment is made and no payments are made thereafter.	N/A	
Existing account with a stable history shows irregularities.	Follow-up, investigate for accuracy.	
An account with low activity unexpectedly jumps to high consumption. Ex: 1000 kwh to 2801 kwh.	N/A	
Mail sent to customer is repeatedly returned.	Check for correct information.	
Customer notifies utility that they are not receiving their bill.	Check for correct information.	
The utility is notified of unauthorized charges or transactions in connection with a customer's account.	Fill out FTC Affidavit by consumer. www.ftc.affidavit	
Notice of Theft		
Utility is notified by law officials or others, that it has opened a fraudulent account for a person engaged in identity theft.	Follow direction of law.	

LVRECC Board Policy Number 233

Effective Date: 03/20/2014

**SUBJECT: IDENTITY THEFT PREVENTION PROGRAM ('RED FLAG')
FACT ACT (FEDERAL REGISTER 16 CFR 681)**

Page 13 of 60

Subsection Number 2

Preventing, Detecting and Mitigating Breaches in Security

Procedure:

1. In the event of a breach of security, the following precautions will be taken to mitigate damage, i. e. files stolen from employee's desk. What are the initial steps?
 - A. Tell supervisor and management.
 - B. Secure information.
 - C. Define and remember what information was stolen.

2. Notification within the utility will follow, i.e. how will the flow of information be told from now? (Describe the order in which designated personnel be alerted?)

Employee shall notify supervisor, supervisor notify management, and management notify privacy officer.

3. Customers affected by the breach will be contacted (Describe the method and time frame for contacting customers affected by the breach)

Notify by phone or mail depending on severity of incident as soon as possible.

4. If there are conditions under which the utility would provide protection coverage for affected customer accounts, describe those conditions.

Get credit insurance to cover affected consumer, depending on severity of incident, for one year once proven there has been a security breach occurrence.

LVRECC Board Policy Number 233

Effective Date: 03/20/2014

**SUBJECT: IDENTITY THEFT PREVENTION PROGRAM ('RED FLAG')
FACT ACT (FEDERAL REGISTER 16 CFR 681)**

Page 14 of 60

Subsection Number 3

Responding to Notices of Address Discrepancies

Procedure:

1. Licking Valley RECC will furnish a confirmed address to the consumer reporting agency (CRA) under the following conditions:
 - A. Utility can form a reasonable belief the consumer report relates to the consumer about whom the user request the report.
 - B. The consumer under review is a current customer with an active account.
 - C. Request involves a customer opening a new account.
 - D. CRA provides request (could be in writing and period of time).
 - E. Utility has established relationship with CRA.
2. Confirmation of address will be provided by utility to CRA. Tell them what time period and how you will give it to them, giving yourself enough time. Do not say 3 minutes; say about 20 to 30 minutes.

Note: the regulations state: "to the extent that such user regularly and in ordinary course of business." Translation - Not requesting a process that will be disruptive.

LVRECC Board Policy Number 233

Effective Date: 03/20/2014

**SUBJECT: IDENTITY THEFT PREVENTION PROGRAM ('RED FLAG')
FACT ACT (FEDERAL REGISTER 16 CFR 681)**

Page 15 of 60

Subsection Number 4

Providing Designated Employees with Identity Theft Prevention Training

Procedure:

1. Designated employees will be trained on a need to know basis according to job responsibilities.
2. **Initial Training** is provided on 3 levels:
 - A. **Committee members** participated in a 12 hour professional association Identity Theft Prevention Program workshop covering principles of needs assessment, program design, development, implementation and evaluation. Strategies for revision and reporting were included. Committee members unable to attend will receive one on one training by a workshop attendee.
 - B. **Supervisors** - Initial 2 hour program addressing supervisory role in preventing identity theft. Go to tab – employee workbook.
 - C. **Employee**- Initial 2 hour program addressing the safeguarding of secured information.
3. **Annual Updates** will be provided for all designated employees. Sessions to be a minimum of 30 minutes will include, but not limited to:

Patterns of incidents, changes in information technology, changes in methods of Identity theft, results of evaluations, seek employee input on strategies for enhancing Identity Theft Prevention Program
4. **Documentation of Training:**

Training will be documented by sign-in sheets with date, time, and attendance.
6. New employees hired into positions handling secured information will receive initial training within 90-days of employment.

LVRECC Board Policy Number 233

Effective Date: 03/20/2014

**SUBJECT: IDENTITY THEFT PREVENTION PROGRAM ('RED FLAG')
FACT ACT (FEDERAL REGISTER 16 CFR 681)**

Page 16 of 60

Subsection Number 5

Handling Reports of Suspected Identity Theft

Procedure:

1. When a consumer suspects identity theft, he must notify the utility in writing, completing the Federal Trade Commission Affidavit. Instructions for completion are a part of the form, and bring FTC and police report to utility.
2. Customer will be requested to submit copy of affidavit with police report.
3. Make a copy of the customer's government issued photo ID.
4. Record the receipt of documents.
5. Submit the copies of the FTC affidavit, police report and photo ID to Privacy Officer.
6. Complete internal investigation and report back to official authorities and affected consumer.

LVRECC Board Policy Number 233

Effective Date: 03/20/2014

**SUBJECT: IDENTITY THEFT PREVENTION PROGRAM ('RED FLAG')
FACT ACT (FEDERAL REGISTER 16 CFR 681)**

Page 17 of 60

NOTICE OF IDENTITY THEFT (LVRECC)

(To be filled out by utility employee)

Party Submitting the Information (Consumer)

Name: _____

Address: _____

Date and Time or Receipt: _____

Verification of Consumer Identity:

Details of alleged ID theft: _____

Signature

Date

I acknowledge receipt of this notice. The information that has been reported as resulting from identity theft:

_____ Has been blocked

_____ Has not been blocked for the following reason(s):

LVRECC Board Policy Number 233

Effective Date: 03/20/2014

**SUBJECT: IDENTITY THEFT PREVENTION PROGRAM ('RED FLAG')
FACT ACT (FEDERAL REGISTER 16 CFR 681)**

Page 18 of 60

Instructions for Completing the ID Theft Affidavit (FTC Form)

To make certain that you do not become responsible for any debts incurred by an identity thief, you must prove to each of the companies where accounts were opened in your name that you didn't create the debt. The ID Theft Affidavit was developed by a group of credit grantors, consumer advocates, and attorneys at the Federal Trade Commission (FTC) for this purpose. Importantly, this affidavit is only for use where a new account was opened in your name. If someone made unauthorized charges to an existing account, call the company for instructions.

While many companies accept this affidavit, others require more or different forms. Before you send the affidavit, contact each company to find out if they accept it. If they do not accept the ID Theft Affidavit, ask them what information and/or documentation they require.

You may not need the ID Theft Affidavit to absolve you of debt resulting from identity theft if you obtain an Identity Theft Report. We suggest you consider obtaining an identity Theft Report where a new account was opened in your name. An Identity Theft Report can be used to (1) permanently block fraudulent information from appearing on your credit report; (2) ensure that debts do not appear on your credit reports; (3) prevent a company from continuing to collect debts or selling the debt to others for collection; and (4) obtain an extended fraud alert.

The ID Theft Affidavit may be required by a company in order for you to obtain applications or other transaction records related to the theft of your identity. These records may help you prove that you are a victim. For example, you may be able to show that the signature on an application is not yours. These documents also may contain information about the identity thief that is valuable to law enforcement.

This affidavit has two parts:

- Part One – the ID Theft Affidavit – is where you report general information about yourself and the theft.
- Part Two – the Fraudulent Account Statement – is where you describe the fraudulent account(s) opened in your name. Use a separate Fraudulent Account Statement for each company you need to write to.

When you send the affidavit to the companies, attach copies (NOT originals) of any supporting documents (for example, driver's license or police report). Before submitting your affidavit, review the disputed account(s) with family members or friends who may have information about the account(s) or access to them.

Complete the affidavit as soon as possible. Many creditors ask that you send it within two weeks. Delays on your part could slow the investigation.

LVRECC Board Policy Number 233

Effective Date: 03/20/2014

**SUBJECT: IDENTITY THEFT PREVENTION PROGRAM ('RED FLAG')
FACT ACT (FEDERAL REGISTER 16 CFR 681)**

Page 19 of 60

Be as accurate and complete as possible. You may choose not to provide some of the information requested. However, incorrect or incomplete information will slow the process of investigating your claim and absolving the debt. Print clearly.

When you have finished completing the affidavit, mail a copy to each creditor, bank or company that provided the thief with the unauthorized credit, goods, or services you describe. Attach a copy of the Fraudulent Account Statement with information only on accounts opened at the institution to which you are sending the packet, as well as any other supporting documentation you are able to provide.

Send the appropriate documents to each company by certified mail, return receipt requested, so you can prove that it was received. The companies will review your claim and send you a written response telling you the outcome of their investigation. Keep a copy of everything you submit.

If you are unable to complete the affidavit, a legal guardian or someone with power of attorney may complete it for you. Except as noted, the information that you provide will be used only by the company to process your affidavit, investigate the events you report, and help stop further fraud. If this affidavit is requested in a lawsuit, the company might have to provide it to the requesting party. Completing this affidavit does not guarantee that the identity thief will be prosecuted or that the debt will be cleared.

If you haven't already done so, report the fraud to the following organizations:

1. Any one of the nationwide consumer reporting companies to place a fraud alert on your credit report. Fraud alerts can help prevent an identity thief from operating any more accounts in your name. The company you call is required to contact the other two, which will place an alert on their versions of your report, too.

Equifax: 1-800-525-6285; www.equifax.com

Experian: 1-888-EXPERIAN (397-3742); www.experian.com

TransUnion: 1-800-680-7289; www.transunion.com

In addition, once you have placed a fraud alert, you're entitled to order one free credit report from each of the three consumer reporting companies, and, if you ask, they will display only the last four digits of your Social Security number on your credit reports.

2. The security or fraud department of each company where you know, or believe, accounts have been tampered with or opened fraudulently. Close the accounts. Follow up in writing, and include copies (NOT originals) of supporting documents. It's important to notify credit card companies and banks in writing. Send your letters by certified mail, return receipt requested, so you can document what the company received and when. Keep a file of your correspondence and enclosures.

When you open new accounts, use new Personal Identification Numbers (PINs) and passwords. Avoid using easily available information like your mother's maiden name, your birth date, the last four digits of your Social Security number, your phone number, or a series of consecutive numbers.

3. Your local police or the police in the community where the identity theft took place. Provide a copy of your ID Theft Complaint filed with the FTC (see below), to be incorporated into the police report. Get a copy of the police report or, at the very least, the number of the report. It can help you deal with creditors who need proof of the crime. If the police are reluctant to take your report, ask to file a "Miscellaneous Incidents" report, or try another jurisdiction, like your state police. You can also check with your Attorney General's office to find out if state law requires the police to take reports for identity theft. Check the Blue Pages of your telephone directory for the phone number or check www.naag.org for a list of state Attorneys General.

4. The Federal Trade Commission. By sharing your identity theft complaint with the FTC, you will provide important information that can help law enforcement officials across the nation track down identity thieves and stop them. The FTC also can refer victims' complaints to other government agencies and companies for further actions, as well as investigate companies for violations of laws that the FTC enforces.

You can file a complaint online at www.consumer.gov/idtheft. If you don't have internet access, call the FTC's Identity Theft Hotline, toll-free: 1-877-IDTHEFT (438-4338); TTY: 1-866-653-4261; or write: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580. When you file an ID Theft Complaint with the FTC online, you will be given the option to print a copy of your ID Theft Complaint. You should bring a copy of the printed ID Theft Complaint with you to the police to be incorporated into your police report. The ID Theft Complaint, in conjunction with the police report, can create an Identity Theft Report that will help you recover more quickly. The ID Theft Complaint provides the supporting details necessary for an identity Theft Report, which go beyond the details of a typical police report.

**DO NOT SEND AFFIDAVIT TO THE FTC OR ANY OTHER
GOVERNMENT AGENCY**

LVRECC Board Policy Number 233

Effective Date: 03/20/2014

**SUBJECT: IDENTITY THEFT PREVENTION PROGRAM ('RED FLAG')
FACT ACT (FEDERAL REGISTER 16 CFR 681)**

Page 21 of 60

ID Theft Affidavit

Victim Information

- 1) My full legal name is

First) (Middle) (Last) (Jr., Sr., III)
- 2) (If different from above) When the events described in this affidavit took place I was known as

First) (Middle) (Last) (Jr., Sr., III)
- 3) My date of birth is

(day/month/year)
- 4) My Social Security number is

- 5) My driver's license or identification card state and number are

- 6) My current address is

(City/State/Zip Code)
- 7) I have lived at this address since

(month/year)
- 8) (If different from above) When the events described in this affidavit took place, my address was

(City/State/Zip Code)
- 9) I lived at the address in Item 8 from _____ until _____
(month/year) (month/year)

LVRECC Board Policy Number 233

Effective Date: 03/20/2014

**SUBJECT: IDENTITY THEFT PREVENTION PROGRAM ('RED FLAG')
FACT ACT (FEDERAL REGISTER 16 CFR 681)**

Page 22 of 60

10) My daytime telephone number is

My evening telephone number is

**DO NOT SEND AFFIDAVIT TO THE FTC OR ANY OTHER
GOVERNMENT AGENCY**

LVRECC Board Policy Number 233

Effective Date: 03/20/2014

**SUBJECT: IDENTITY THEFT PREVENTION PROGRAM ('RED FLAG')
FACT ACT (FEDERAL REGISTER 16 CFR 681)**

Page 23 of 60

Subsection Number 6

Conducting IT Audits to Monitor Risk for Identity Theft

Procedure:

1. Licking Valley Rural Electric Cooperative Corporation will utilize the Identity Theft Prevention.

Program checklist to audit and evaluate internal and external identity theft risk in information technology security.
2. Walk through inspections will be completed on a quarterly basis by management and complete audits will be completed on a yearly basis by management.
3. Recommendations to reduce risk of identity theft will be submitted for program review and evaluation upon completion of an audit checklist. Results will be submitted to the privacy officer within 90 days from completion of the evaluation.

LVRECC Board Policy Number 233

Effective Date: 03/20/2014

**SUBJECT: IDENTITY THEFT PREVENTION PROGRAM ('RED FLAG')
FACT ACT (FEDERAL REGISTER 16 CFR 681)**

Page 24 of 60

Subsection Number 7

Confidentiality of Medical Records

Procedure:

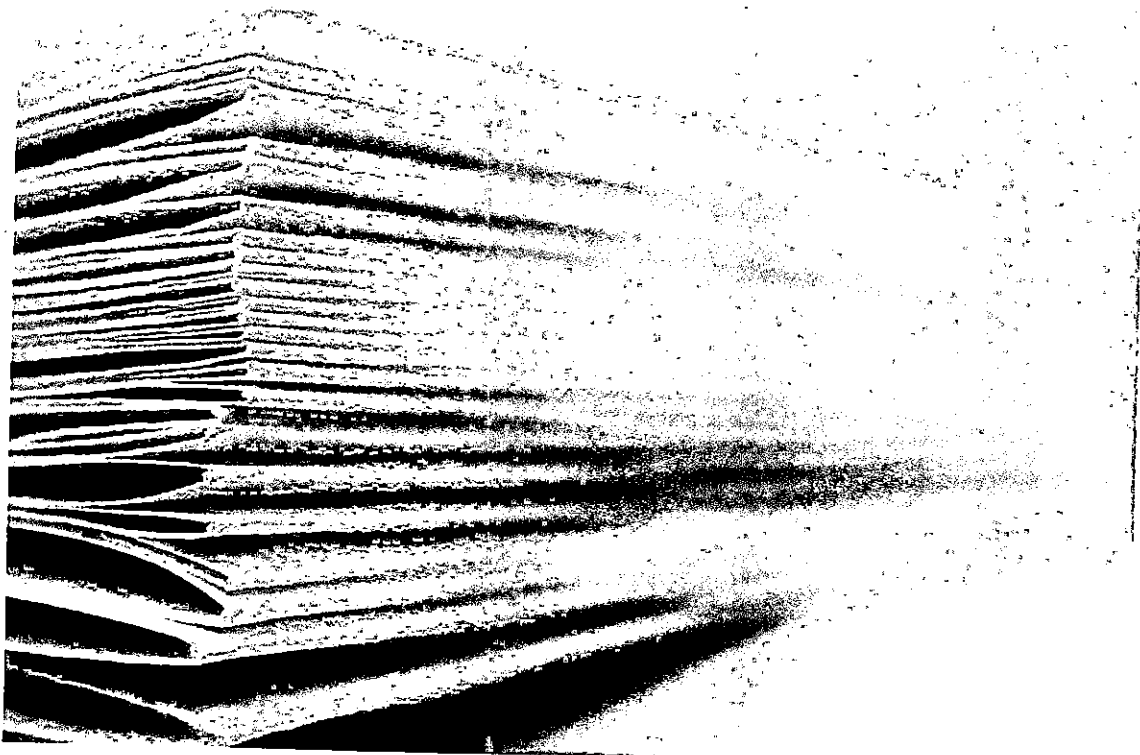
1. Licking Valley Rural Electric Cooperative Corporation will treat all medical information pertaining to the customer as confidential.

Definition:

Medical Information is information or data, whether oral or recorded, in any form of medium, created by or derived from a health care provider or the consumer that relates to:

- The past, present, or future physical, mental, or behavioral health care to an individual;
 - The provision of health care to an individual; or
 - The payment for the provision of health care to an individual
2. Medical information will not be used in the determination of a consumer's eligibility for services.
 3. Licking Valley Rural Electric Cooperative Corporation will not release medical information to third parties.
 4. Rescue Squads, government entities that require the location of citizens on ventilators for **planning** purposes will be provided the information upon the written permission of the customer.

Identity Theft Prevention Programs in American Utilities: Guidelines for Compliance with Red Flags



Provided by Tennessee Valley Public Power Association

Employee Workbook for Safeguarding Customer Information

Dedication

This program is dedicated to the thousands of utility workers who relentlessly serve. You do not get to choose who will be your customer. As a result, you serve all sides of humanity. The kindness and respect you show to those, who have not been so generous with you, is perhaps your most remarkable accomplishment of all.

Copyright 2008 TVPPA All rights reserved. No portion of this book may be reproduced, stored in a retrieval system or transmitted in any form or by any means-electronic, mechanical, photocopy, or any other without the permission of the publisher.

Red Flags Employee Training

It Takes a Thief

To begin this training, you are going to look at the world through the eyes of a criminal. Imagine being in and around your utility on the lookout for secured information (Social Security Number-SSN, driver's license, Date of Birth-DOB, address, name, etc.). You have a notebook and a brief case. Let's see what you can find.

In the parking lot, you find an unlocked company vehicle with a laptop. Quickly, stick it in your briefcase. You overhear a customer at the drive up window tell the CSR his name, address, and date of birth. The CSR repeats the information back to him. You have written it down in your notebook. Good work. A look around the dumpster reveals half of a crumpled application that has what looks like coffee on it. On the barely readable paper is a name, address, date of birth, social security number and place of employment. Now you are getting somewhere. Take this stuff home. You have too much to run a risk. From a phone at the customer's place of employment, call the bank and ask about last payment. "I think I might have paid that bill twice – What is the last check number you show? My husband keeps so many accounts. Is that the First American Account or Regency Bank?"

This is just too much fun. Now you are going back to see what you can find when you go inside the doors. First, write down any information in the area where new accounts are opened. If the CSR leaves his desk, look in the trashcan for notes, on the desk for files and quickly put them in your brief case. If there are any access codes or passwords taped or on a sticky note on the monitor, write them down in your notebook. You have a buyer for that stuff. Search any area for abandoned monitors that still have social security information on the screen. Hey wait this desk has the access code numbers taped under the work area. Who do they think they're kidding? It just does not get better than this. Now let's look for purses. It takes a little time, but you just found the purse of a new employee. Wow, real leather; at least our victim has nice taste.

Back at home camp, you check inside the purse: a cell phone, driver's license, social security card, ATM card, checkbook and pictures. You text her husband saying, "I forgot the pin number!" If he gives it to you, respond thanks and celebrate. You have just completed your first morning of life as a thief. Not bad.

In order to protect our customers from identity theft, we have to be one step ahead of thieves. In each of the above situations, how could the utility employees better protect the information?

Introduction:

In the time it takes to read this first sentence there will be four (4) new victims of identity theft in the United States.

The fastest and most financially devastating crime in the United States is identity theft. The emotional and financial cost to the victim can affect their quality of life. In a utility, breaches in information security, lessen the trust the public must place on us to establish the power supplier/consumer relationship.

I. How Legislation is Changing the Way We Monitor and React to Possible Signs of Identity Theft or Red Flags.

The FACT Act (2003) was passed to set standards for guarding customer information. On November 1, 2007, the red flags were added to hold businesses liable for the prevention, detection and mitigation of identity theft.

Does your utility daily procedures support consumer privacy?

A. Why Utilities?

- Because utilities maintain on going accounts primarily for personal, family or household purposes.
- The accounts are designed to accept multiple payments.
- Utilities are the site for a large portion of identity theft crime in the United States.

B. Are We Responsible to Our Members/Customers?

In a word, yes. The utility has the responsibility of developing an identity theft prevention program to protect our customer's personal information. The FACT Act outlines the requirement to:

DETECT

PREVENT

MITIGATE¹

C. Where Do We Begin?

- Make a list of red flag indicators of identity theft drawn from experience in the utility industry. In other words, what has been the past and current patterns used to gain services under a stolen identity?
- What proactive strategies can be incorporated into our day to day policies and procedures that will discourage or detect identity thieves?

¹ Control damage done

D. *How Do We Add One More Thing On Our Plate?*

In the utility industry, a strong sense of providing reliable service has always been evident. We provide a critical service that our customers need to sustain everyday life. The dedication to protecting and serving "the little lady at the end of the line" has always been a part of our culture.

The Identity Theft Prevention Program is another step in the direction of providing service for our customers. Protecting a customer's personal identity information is indeed our lawful responsibility.

Effective business practices and policies that spot attempted and actual identity theft early have great potential for relieving the national crime wave. Identity thieves often establish cell phone and utility (established proof of residency) accounts in the victim's name.

Utilities suffer significant losses from customers who use stolen identities for service and walk away from large bills. Careful validation of identity in the process of opening an account and the use of red flags (such as alerts) has already been demonstrated to minimize losses. Proper screening of new and existing accounts not only protects secure information but also is an effective approach to keeping the cost per kilowatt-hour within reach of the working family.

What is a red flag?

A pattern, particular specific activity that indicates the possible risk of identity theft.

A red flag triggers the need to investigate, gather facts and mitigate.

Examples:

- A consumer fraud alert or active duty alert
- Any account that would adversely affect a consumer's credit standing should be considered at risk of identity theft and thus subject to a red flag
- An address discrepancy reported by a consumer reporting agency
- A consumer's communication about attempted or actual identity theft
- A company's knowledge of a security breach within its own confines or that of an affiliate with which the company has shared data
- Attempts to open new accounts with altered documents
- Suspicious actions by employees – downloading customer account information being added to customer account

It is important that red flags be treated as examples of indicators of possible theft and not defacto evidence of identity theft.

The vast majority of identity theft in the utility industry has historically been within families. There is no reason to doubt that trend will still occur. There is, however, a much more dangerous threat developing throughout the US. Professional or maybe we should just say very effective thieves, will usually establish proof of residency with a

utility bill. Our government is asking us to not only protect our customer's secured information, but be a part of the answer to the problem. Remember, *it is not our job to accuse, only to report. Being consistently kind and respectful is always the right thing to do. This will keep make the environment safer for us and we will be less likely to accuse someone who is innocent. You may also find that the detective or police officer in your area does not want a potential suspect to be forewarned.*

E. Identity Theft versus Identity Fraud

Identity fraud occurs when someone gives you fictitious information such as:

- a social security number that has never been issued.
- an address that does not exist.
- the name of a person that does not exist.

In this case the utility has the option to respectfully request additional before beginning services. A potential victim has not been established.

Identity theft occurs when someone gives you fraudulent information such as:

- social security number issued to another individual.
- social security number listed on death file.
- name and address belonging to someone else.

In this case, the suspicion of a potential victim has been established.

Identity theft is a much more serious problem. Identity theft is when someone gathers personal information and assumes a new identity as their own. This can include getting seemingly authentic forms of identification using real or fake "breeder" documents (a breeder document is a document used to establish identity for other forms of ID; for example, presenting a birth certificate to the department of motor vehicles to get a drivers license). With their new identification in hand, criminals perpetrating an actual identity theft can then open new accounts, apply for loans or mortgages, and generally make a very big, expensive mess of the victim's life.

Case No. 1

Title: "Stolen Identity"

In the public power industry, over 50% of all identity theft occur within families.

A sister in Middle Tennessee used a social security number that belonged to her sister that lived in Kentucky. She is able to obtain fraudulent picture identification in her sister's name. She opens a new water, gas, electric and cable account at the local municipality. While she paid the initial deposit, her bills are being returned by the post office. She has made no attempt to make any payment at 60 days. A service man is sent to warn her about the cut off date and tells him she would be more than happy to pay. She explains she needs the bills in writing because her father in Texas is paying them for her. The accounting office grants her an additional 30 days to complete all transactions with the condition that all accounts will be current by the 10th of the month. On the 8th, she has a church organization working to help her raise the funds. On the 11th, the sister in Kentucky sees the activity on her credit report. Her sister has had a life long habit of manipulating family members to survive. For years they followed her from state to state cleaning up the mess. The sister in Kentucky calls the utility and alerts them of the fraudulent use of her identity.

Topics of Discussion:

- 1. How would you verify the facts? How will we establish "reasonable basis" for identity?**
- 2. When you have confirmed that she has stolen her sister's identity, how will you proceed?**

Case No. 2

Title: *Mrs. B*

Mrs. B sent her 10 year old grandson, John, a check for his birthday. John's parents have recently divorced on bad terms. His father sees the check in John's book bag on a scheduled visit and copies down the routing number and checking account number. He uses the information to call in utility payments for the next three months. Mrs. B realizes the theft when her sister comes by to help her manage her account. She is embarrassed, by her former son-in-law's behavior, but does not want to be held accountable for the \$721.00 in charges and late fees. The Utility is notified of the son in law's intent of fraudulent use of Mrs. B's banking account.

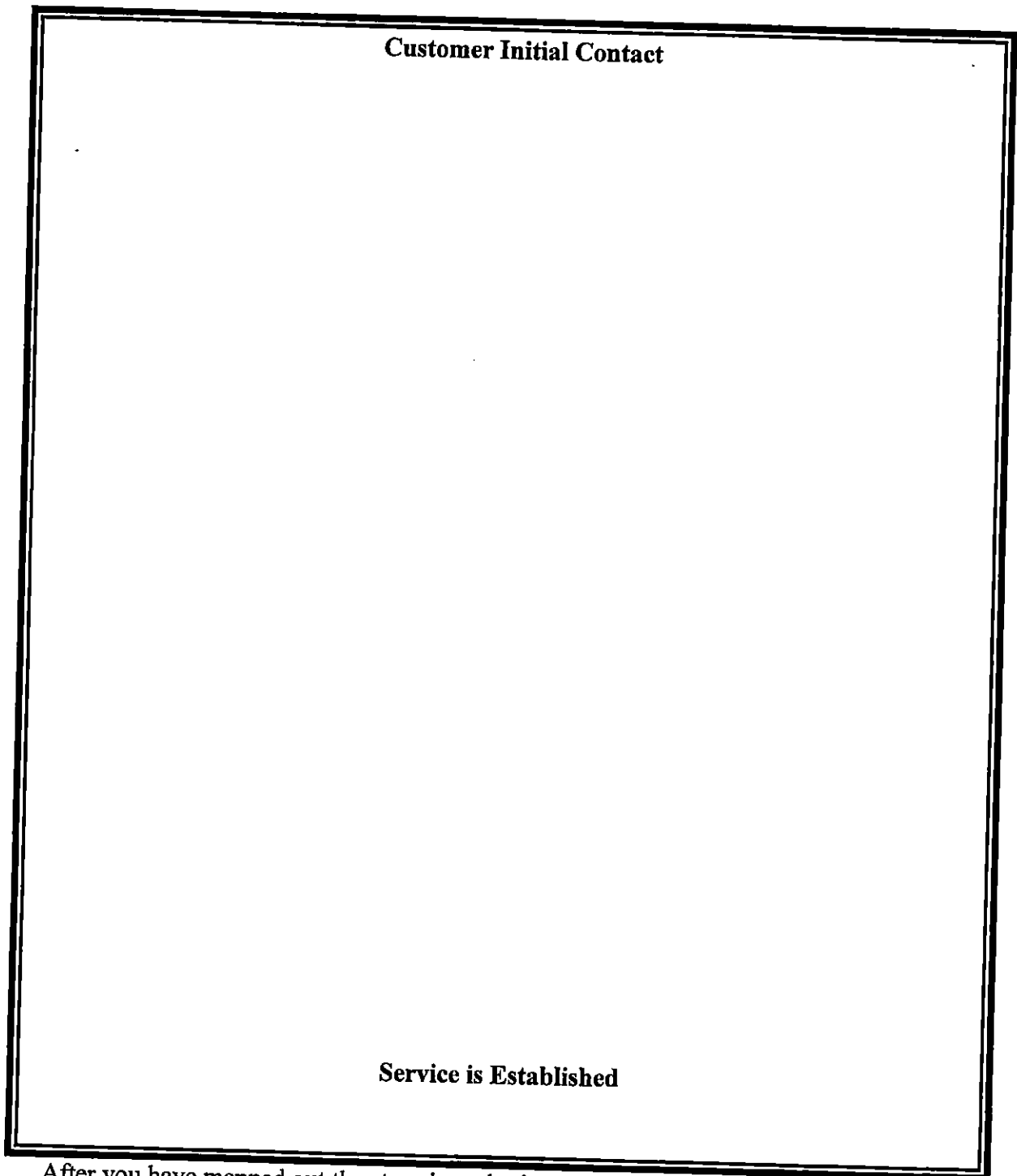
Topics of Discussion:

- 1. Could this theft have been detected before Mrs. B. called? How?**
- 2. Do you think it is possible that Mrs. B has cleaned up the financial messes made by this man before?**
- 3. How should the Utility handle the current situation?**
- 4. What can the Utility do to prevent a repetition?**

F. Red Flags Checklist and Review for Utilities

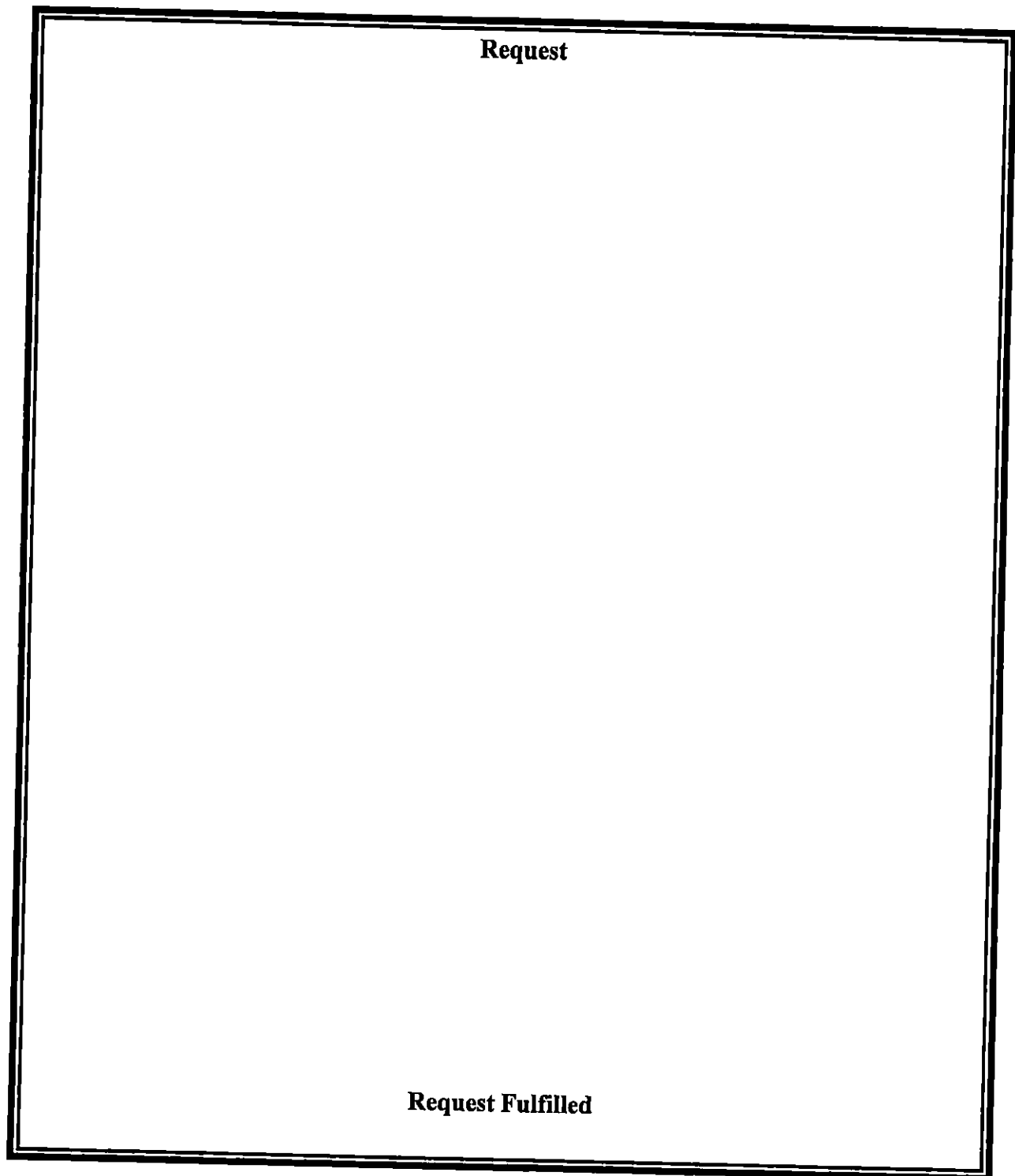
Alerts, Notifications or Warnings from Consumer Reporting Agency	Suspicious Documents	Suspicious Personal I.D. Information	Unusual Use or Suspicious Activity related to the Covered Account	Notice of Theft
1. A fraud or active duty alert is included with a consumer report.	5. Documents provided for ID appeared altered or forged	10. Personal ID is inconsistent with external information sources: addresses do match consumer report/ or social security (SS) number has not been issued or is listed on the SS Administration Death Master File	19. Change of billing address is followed by request for adding additional properties to the account (or shortly following the notification of a change in address, the utility receives a request for the addition of authorized users on the account.)	26. Utility is notified by law officials or others, that it has opened a fraudulent account for a person engaged in identity theft.
2. Consumer reporting agency provides a credit freeze on the customer report	6. The photo or physical description is not consistent with the appearance of the applicant	11. Personal ID given by customer is not consistent with other personal ID info. Ex: There is a lack of correlation between the SSN# range and DOB	20. Payments are made in a manner associated with fraud. For example, deposit or initial payment is made and no payments are made thereafter.	
3. Consumer Reporting Agency provides a notice of address discrepancy	7. Other information given to open the new account is not consistent with the ID of the applicant	12. Personal ID provided is associated with known fraudulent activity. Using same addresses and or phone numbers	21. Existing account with a stable history shows irregularities	
4. A consumer report indicates a pattern of activity that is inconsistent with the story and usual pattern of activity of an applicant or customer such as :	8. Other information on the identification is not consistent with readily accessible info on file such as signature or recent check.	13. Personal ID is of the same type associated with fraudulent activity: fictitious address, mail box drop, or prison or phone number is invalid; it is associated with a pager or answering service.	22. An account with low activity unexpectedly jumps to high consumption.	
a. recent or significant increase in the number of inquiries	9. An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.	14. The SS# is the same as customers opening other accounts.	23. Mail sent to customer is repeatedly returned.	
b. an unusual number of recently established credit relationships		15. The address or phone number is the same as a large number of other applicants.	24. Customer notifies utility that they are not receiving their bill.	
c. a material change in the use of credit especially with respect to new established credit relationships		16. The customer fails to provide all needed personal ID upon request.	25. The utility is notified of unauthorized charges or transactions in connection with a customer's account.	
d. an account that was closed for cause or identified for abuse of account privileges		17. Personal ID is inconsistent with utility records.		
		18. For institutions using challenge questions, the person attempting to access or open the account cannot provide any information beyond what would typically be found in a wallet or consumer report		

Step 1 – Map out the steps that occur for processing a new account.



After you have mapped out the steps in gathering customer information to start a new account, highlight the areas where red flags might possibly appear.

Step 2 - Map out the ways customers, 3rd parties and others access existing accounts.



After you have mapped out the flow of information, highlight the possible areas where a red flag could occur.

Discuss with your supervisor, what is the policy in you utility in the event of:

Employee Responses Include:	
Alerts:	
<ul style="list-style-type: none"> • Fraud • Credit Freeze • Notice of Address Discrepancy • Unusual Pattern of Activity 	
Suspicious Documents:	
<ul style="list-style-type: none"> • ID altered or Forged • Photo or description does not match customer • Inconsistent information • Paperwork appears to have been forged or altered, destroyed and reassembled 	
Suspicious Personal ID Information:	
<p>ID inconsistent with external sources:</p> <ul style="list-style-type: none"> • Address does not match consumer report • SS# given has not been listed or is on the SS Adm. Death Master File • ID info conflicts such as SS# and DOB Information given is associated with fraudulent activity • SSN is same as other customers • Address is same as other customers • Customer fails to provide all ID requested • Personal ID is inconsistent with utility records 	
Unusual User or Suspicious Activity:	
<ul style="list-style-type: none"> • Change of billing address is followed by authorization of additional users • Deposit is made and no payments are made there after • An existing account with a stable history shows irregularities • Mail sent to customer is repeatedly returned • Customer notifies utility that they are not receiving their bill 	

Notice of theft:

- Utility is notified of unauthorized charges or transactions in connection with a customer's account

Case No. 3

Title: *Kentucky Consumer*

"My 9 year old daughter was a victim of identity theft through this organization. Someone used my daughter's Social Security Number to obtain unauthorized utilities in her name. (The) utility was unwilling to assist in my daughter's case in bringing the perpetrator to justice. The (utility company) informed me that they do not run checks on identification showed to them to ensure validity. The (utility company) informed me that it is easier and cheaper to write off utility losses then to investigate and prosecute cases of utility fraud/identity theft. I feel that this exemplifies poor public security and displays ineptness towards individual rights. My daughter was a victim and I am sure there are many more that will be victimized as long as companies refuse to stand up for laws that protect us." (This story posted online on 9/22/04)

Topics of Discussion:

- 1. Why do you think utilities tend to write off losses vs. investigate and prosecute?**
- 2. Why are children a target for stolen social security numbers?**
- 3. Does the customer have a right to feel "protected?"**

What is your role in the utility's identity theft prevention program?

Due diligence with regard to protecting customer information

This includes your own daily habits:

- ✓ Disposing of records or paper with notes
- ✓ Taping access information around work station
- ✓ Speaking in a manner that allows others to overhear secured information
- ✓ Leaving your work area with the monitor on, files on desk, customer information in view of others
- ✓ Sharing passwords, access codes, etc
- ✓ Discussing personal information regarding a customer with other employees. Information is shared only on a "Need to Know" basis.

Carefully monitor your work area

If someone implies they are with an outside vendor authorized to access your equipment, verify first with your supervisor.

Watch for unusual behavior, employees downloading large amounts of information, unauthorized personnel or citizens in areas with secured information.

Validate identification for new and existing accounts. Check documents.
Our customers do have a right to feel protected.

Utility employees are not required or encouraged to confront individuals suspected of committing a crime. It is our lawful obligation to report to the police any "suspected" patterns of identity theft. It is the responsibility of the detective or officer working in identity theft to do the investigation. The laws regarding reporting identity theft are similar to reporting child abuse. You report when there is a suspicion. It is up to law officials to determine if a crime has actually been committed.

LVRECC Board Policy Number 233

Effective Date: 03/20/2014

**SUBJECT: IDENTITY THEFT PREVENTION PROGRAM ('RED FLAG')
FACT ACT (FEDERAL REGISTER 16 CFR 681)**

Page 40 of 60

Validating Customer Identity

Licking Valley Rural Electric Cooperative Corporation in compliance with the CIP rules of the Patriot Act will make every attempt to validate the identity of consumer applying for service or seeking to make request on an existing account.

Identification Required		Validation Method	Exceptions (If any)
Methods Provided to Open Account			
In Person	Social Security Card Photo ID or Drivers License (A minimum of 2 forms of ID)	Look at Picture, Signature, Date of Birth, Social Security Card – 3 rd Party to validate only. Signature(s) on every work order (disconnects, new connects, reconnects, name changes, etc.)	Will not give Social Security Card, then must have Birth Certificate, Military ID, Passport, or Green Card.
By Phone	N/A	No new work orders over phone, even out of state.	If existing out-of-state consumer only, give last 4 digits of Social Security Number.
By Electronically	N/A		
By Other		If no ID and well known, leave up to supervisor. The serviceman can check ID, if disabled person.	

Identification Required		Validation Method	Exceptions (If any)
Methods Provided to Access Existing Account			
In Person	Asking for printouts. If person is not known, need to ask for Drivers License.		
By Phone	Account Number or last 4 digits of Social Security Number.	Address	
By Electronically			
By Other			

New Services will be denied if proper identification is not provided.

Request for access or change on account will be denied if proper identification is not provided.

LVRECC Board Policy Number 233

Effective Date: 03/20/2014

**SUBJECT: IDENTITY THEFT PREVENTION PROGRAM ('RED FLAG')
FACT ACT (FEDERAL REGISTER 16 CFR 681)**

Page 42 of 60

Reporting/Revision/Updates

Licking Valley Rural Electric Cooperative Corporation has established a Privacy Committee to meet on a Licking Valley Rural Electric Cooperative Corporation basis. The purpose of the meeting will be to evaluate:

- Incidents involving identity theft and management's response.
- Effectiveness of policies and procedures.
- Recommendations for changes in the program.

Risk will be evaluated along with recommendations for improvement and submitted to the Board of Directors on an annual basis.

Incidents will be recorded as they occur by utility employees and reported to the Privacy Committee. The incident record form is designed to provide the following as information is available: date, description of significant event, management response, scope, mitigation employee, employee red flag training record. The Committee will review patters every 6 months. A portion of the Annual Report will represent a summary of the incident record. Additional sections of the report will include, but not be limited to material changes in the program, current assessment of strengths and areas for improvement as well as program goals for the coming year.

LVRECC Board Policy Number 233

Effective Date: 03/20/2014

**SUBJECT: IDENTITY THEFT PREVENTION PROGRAM ('RED FLAG')
FACT ACT (FEDERAL REGISTER 16 CFR 681)**

Page 43 of 60

**Identity Theft Prevention Program Incident Report
Licking Valley Rural Electric Cooperative Corporation**

Date:

Prepared by:

(Employee designated to track and record information)

Committee Members:

It is the policy of Licking Valley Rural Electric Cooperative Corporation to provide an Identity Theft Prevention Program for customers and employees. The purpose of this report is to promote continued evaluation of effectiveness of current policies and procedures in compliance with the FACT Act (2003). This document will be used to drive recommendations for changes to the program due to evolving risk and methods of theft.

PRIVACY COMMITTEE SUMMARY FORM

Exhibit 1
Page 45 of 61

Date	Scope	Employee	Employee Trained	Describe Incident or "Significant Event"	Management Response	Mitigation

LVRECC Board Policy Number 233

Effective Date: 03/20/2014

**SUBJECT: IDENTITY THEFT PREVENTION PROGRAM ('RED FLAG')
FACT ACT (FEDERAL REGISTER 16 CFR 681)**

Page 45 of 60

**Identity Theft Prevention Program Incident Report
Page 3**

Describe current strengths of Utility Identity Theft Program.

Describe areas for Improvement.

Goal for Improvement	Steps Needed	Person(s) Responsible	Date

LVRECC Board Policy Number 233

Effective Date: 03/20/2014

**SUBJECT: IDENTITY THEFT PREVENTION PROGRAM ('RED FLAG')
FACT ACT (FEDERAL REGISTER 16 CFR 681)**

Page 46 of 60

Committee Signatures

(Name) (Title) (Date)

(Name) (Title) (Date)

**Identity Theft Prevention Program Red Flags Implementation Checklist for
Utilities**

Privacy Officer: _____

Committee Members: _____

Management Infrastructure

Question	Comment	Yes/No Date
Has a privacy officer and committee been established?		Yes 03/20/2014
Does the committee have representations from at least 3 key areas?		Yes 03/20/2014
Are defined responsibilities outlined for committee members?		Yes 03/20/2014

Question	Comment			Yes/No Date
Is there a written identity theft prevention plan?	In process.			Yes 03/20/2014
Does the written plan provide a policy/procedure for: (Note – you can incorporate existing policies into your program)	Utility Policy Complies No	Utility Policy Next Revision No	Write Policy Yes 03/20/2014	
1. Preventing/Identifying and Mitigating Red Flags	No			
2. Handling a breach in security	No			

Question	Comment			Yes/No Date
3. Record Disposal				Yes 03/20/2014
4. Customer Request Records				Yes 03/20/2014
5. IT security internal	CIS provided			Yes 03/20/2014
6. IT security external	CIS provided			Yes 03/20/2014
7. Screening/Hiring and Training Key Employees handling sensitive information	Utility Policy Complies No	Utility Policy Next Revision Yes	Write Policy Yes 03/20/2014	
8. Privacy Officer/ Committee Members roles/ terms of service/ method for appointment	No	Yes	Yes 03/20/2014	
9. Program assessment and revision				Yes 03/20/2014
10. Program reports tracking incidents & resolutions - Report to General Manager and Board of Directors				Yes 03/20/2014

Question	Comment			Yes/No Date
Utility has requested from local identity theft police officer/detective: Reporting procedures and document training	Name of Contact: Contact Info:			No
All current employees involved in handling sensitive information have received identity theft prevention training/red flags	Names of Employees	Date Trained	Trainer	No
Human Resources has incorporated the identity theft prevention skills in the:	N/A			
orientation	N/A			
and performance evaluation of key positions.	N/A			
Employees' sign Security Agreement (Are all staff informed of the consequences of breaking security regulations?)	N/A			

Question	Comment	Yes/No Date
IDTPP updates are provided on a continual basis to key employees: trends in theft, legislation, IT as well as best practices/mitigation procedures		Yes
Procedures for employees as they leave the utility	There are many things to clean up in IT systems to remove their authorities	No
Consultants sign written 3 rd party contracts which outline the consequences of breaking security regulations		Yes
Are there any routines for the end of assignments	Clean IT system to remove the consultant's authority	No
Information Classification		Yes
Is there a system for information classification according to the appropriate level of availability? (e.g. open, confidential, secret)	To make it possible to apply the most effective security measures.	
Does the classification system require encryption for any class or type of information?		Yes
Is there a classification checklist to make it easy for the user to determine information class?		No
Software		No
Are there any instructions for bringing outside software/data into the utility?		

Question	Comment	Yes/No Date
Are policy documents and security guidelines considered during developing systems?	Security features must be implemented from the beginning.	Yes
Are security requirements included in the demand specification when buying or developing systems?	The requirements must be included from the beginning.	Yes
Are system tests and development separated from production systems?	Avoid compilers and editors in production systems. (More vulnerable to hackers is able to compile in production)	Yes
Are security-related patches from developers and/or vendors implemented as soon as possible?	Routine will include a download to a test environment.	Yes
Is a security validation approval done before introducing new software? Individual users should not be allowed to introduce new software.	New software might create new holes in the system. For example employee may download a game which contains a keystroke logger. Information is sent to the hacker.	No
Is there a routine for installing a new operating system?	This is the most critical software and all configuration parameters must be checked before rebooting.	No
Is it a classified operating system?	According to ITSEC, TCSEC, Common Criteria	Yes
Are security options in the operating system activated?		Yes
Are there any routines to change all security related default parameters in the operating system?	Security if determined by server when computer joins the network	Yes
Is it the same type of routine for application software?	To change defaults and to set security parameters.	Yes
Are additional (e.g. hacks) and self-developed software well documented?	If system crashes, security procedures outline steps for getting the system back up.	Yes

Question	Comment	Yes/No Date
Are there any routines to request all patches that are needed to preserve the security?	To prevent hacking possibilities. (Note Patch = Repair to Program)	Yes
Are 'system-tools' protected?	Software to administer and service the system.	Yes
Are the use of 'system tools' restricted to just a few persons?		Yes
Is all use of 'system-tools' logged?		Yes
Is anti-virus software installed and activated?		Yes
Do the users know how to handle viruses?		Yes
Are there any extended controls of software downloaded from WAN such as Internet?		No
Are the users informed about software licenses, as to what extent they are allowed to copy them and use them in other equipment? If they are allowed to use them for private use at home, etc.?		Yes
Is loading of new software regulated?		Yes
Is critical software backed up and stored in another safe place?		Yes
Is critical software protected by checksums?		No
Is all software from well-known sources?	Special notice on encryption software.	Yes
Hardware		No
Are there any instructions for bringing equipment outside the organization?		
Are there instructions on how to discard equipment?		No
Is it made clear that the		Yes

Question	Comment	Yes/No Date
equipment is for business use only and not for private use by the user?		
Are policy documents and security guidelines considered during introduction of new equipment?		Yes
Are security requirements included in the demand specification when buying or changing equipment?	The requirements must be included from the beginning.	Yes
Is a security validation made before introducing new hardware?	New hardware might create new holes in the system.	Yes
Is there a person responsible for each workstation/personal computer?		Yes
Do the laptops used for field work-mapping software-also contain customer personal ID info? How is ID protected?		Yes
Documentation		No
Is the management policy document printed and distributed to all members of staff and subsequently to new members?		
Is there an Information Security handbook?		No
Are systems and manual routines well documented?	To prevent the dependence on key-persons.	No
Are there documents describing: <ul style="list-style-type: none"> • Hardware • Software • Applications • Communication Are they up to date?		No

Question	Comment	Yes/No Date
Do handbooks for each staff category exist? • Developer • Administrators (network, database etc.) • Users • Helpdesk • Etc.		No
Are there written rules defining responsibility and authority for each staff category?		No
Are system documents stored in a safe place?		Yes
Do security logs track log ins, users and application?		No
Computer Media		Yes
Are there any routines for labeling media?		
Is the existence of media checked on a regular base?	Media in the inventory list.	Yes
Are there any routines to handle missing media?		No
Are there any routines for archiving media?	Back up server on nightly basis and archive.	Yes
Are there any routines for transporting and storing media?		No
Are there any routines for destroying media?	Degauss tape Break CDs	No
Are there any routines for how to handle media during service?	Don't leave media unattended during service and don't let media with secret information leave your organization.	No
Identification and Authorization		
Does the system include logging and alarm functions? For example is someone attempts to log in 3 times unsuccessfully, is a message sent to the network administrator?		No

Question	Comment	Yes/No Date
Does the system include access control to resources/objects?		Yes
Is it quality tested on password/PIN?	Minimum of 8 characters with at least 3 alphabetic or numeric characters mixed.	Yes
Is it possible to reuse old passwords/PIN?	Should not be.	Yes
Is it possible to use the user ID as password/PIN?	Should not be.	No
Are there any routines to change software default passwords?	Upon installation, is the software default password changed?	No
Is the number of log in attempts limited?	Should be to prevent hacking.	No
Is the change of password/PIN compulsory after a certain number of days?	Do employees tape passwords or pin numbers to monitor or under desk area?	No
Does the system block an account if the password is not changed within the time limit or the account has been remained unused?	Should be.	No
Is it possible for a user to change their privileges?	Should not be.	No
Is the password/PIN encrypted? (one way encryption)	Should never be transported or stored in an unencrypted way.	Yes
Is the password/PIN individual?	Must be.	Yes
System Security		Yes
Is there a routine to ensure the correct date and time in all systems and are they synchronized?		
Are there enhanced logging facilities in critical systems?		No
Are there documented procedures for changing the network?		No
Are all changes to the network documented?		No
Are open ports on HUB		No

Question	Comment	Yes/No Date
blocked?		
Is the network administrator privilege restricted to a few users?		Yes
Is all network hardware (HUB, Repeaters, Routers, Gateways, etc.) well protected?		Yes
Is the software in the network hardware well protected? Use strong authentication for changing the software or configuration.		Yes
Internal Protection Is an IDS (Intrusion Detection System) installed?	Alerts system administrator	Yes
Protection from Outside Sources Is a firewall installed?		Yes
Is there a routine for the administration of the firewall?	Setting up a firewall is not a once-and-for-all job. It must be updated constantly.	No
Is the use of encryption considered?	Is there a trustworthy algorithm and key administration?	No
Is access to communication ports for service protected?		No
Are the safeguards (including encryption when needed) considered regarding: <ul style="list-style-type: none"> • Email • FTP • PPP • EDI • SNMP • DNS –services • Routing • Java, Javascript • ActiveX 	<p>File transfer protocol</p> <p>Electronic Data Interchange</p> <p>Domain Name services will affect web site, lotus notes, mail server</p>	Yes

Question	Comment	Yes/No Date
<ul style="list-style-type: none"> • Finger • Rlogin • Cookies 		Yes
Are VPN (Virtual Private Networks) used?		Yes
Logging		
Are the log files protected against unauthorized access?		Yes
Is the system configured in a way that the log must be turned on?		Yes
What events are logged: <ul style="list-style-type: none"> • Login • Logout • Failed login • Exceptional behavior 	User not acting normal. Might be sorted out via IDS. Employee downloads an extraordinary number of customer records into their personal file.	No
<ul style="list-style-type: none"> • Access violation Activities in the Identification and Authorization system?	Unauthorized access to resources. New users, change of privileges, remove of users, etc	No
Physical Protection		No
Are all premises protected?		No
Are computers and network components placed in an access protected area?		No

Question	Comment	Yes/No Date
Is all system documentation safeguarded?		No
Are communication lines protected?		No
Is there an admission and leaving control system with a log?		No
Server room is under lock and key.		No
Is there an up to date list with authorized people?		Yes
Incident handling		Yes
Is there a plan for how to handle incidents?		03/20/2014
Contingency planning		Yes
Is there a contingency plan? How to recover the system after an incident?		

LICKING VALLEY RURAL ELECTRIC COOPERATIVE CORPORATION

KENTUCKY 56 MORGAN

BOARD OF DIRECTORS POLICIES AND PROCEDURES MANUAL

Policy Number 233

Effective Date: 03/20/2014

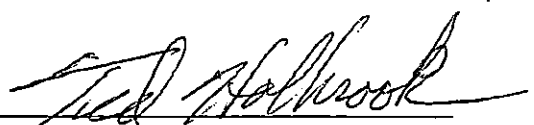
**SUBJECT: IDENTITY THEFT PREVENTION PROGRAM ('RED FLAG')
FACT ACT (FEDERAL REGISTER 16 CFR 681)**

Page 59 of 60

This Policy supersedes all prior policies with number 233.

Board Approved March 20, 2014

Secretary



ID Theft Affidavit

Victim Information

- 1) My full legal name is

(First)

(Middle)

(Last)

(Jr., Sr., III)

- 2) (If different from above) When the events described in this affidavit took place I was known as

(First)

(Middle)

(Last)

(Jr., Sr., III)

- 3) My date of birth is

(day/month/year)

- 4) My Social Security number is

- 5) My driver's license or identification card state and number are

- 6) My current address is

(City/State/Zip Code)

- 7) I have lived at this address since

(month/year)

- 8) (If different from above) When the events described in this affidavit took place, my address was

(City/State/Zip Code)

- 9) I lived at the address in Item 8 from _____ until _____
(month/year) (month/year)

- 10) My daytime telephone number is

My evening telephone number is

**DO NOT SEND AFFIDAVIT TO THE FTC OR ANY OTHER
GOVERNMENT AGENCY**

LICKING VALLEY RURAL ELECTRIC COOPERATIVE CORPORATION

KENTUCKY 56 MORGAN

BOARD OF DIRECTORS POLICIES AND PROCEDURES MANUAL

Policy Number 235

Effective Date: 04/21/2016

SUBJECT: PRIVACY POLICY

Page 01 of 05

PURPOSE: Licking Valley Rural Electric Cooperative Corporation respects the privacy and confidentiality of member information. This policy describes the information that LVRECC collects from its members as a routine part of its operations and how it uses, protects and shares the information that it collects.

POLICY: The Cooperative's

RESPONSIBILITIES: The General Manager/CEO is responsible for the general administration or cause to have performed by his/her staff.

The implementation of the practices, as set forth in this policy is delegated to each department head with prior approval of the General Manager/CEO, to include the responsibility for exercising sound judgment and equitable treatment.

PRACTICES: A. **Categories of Information Collected**

1. Contact information, including a member's name, address, telephone number and e-mail address. Licking Valley Rural Electric Cooperative Corporation might also collect a user name and password for online access.
2. Billing information, including Social Security number, credit information, financial account information and payment history.
3. Electric usage data gathered by LVRECC's metering systems and a member's service history which may include information on a member's property and appliances and information maintained for meter reading purposes (e.g., warning about a dog in the yard, meter tampering, etc.).
4. Capital and patronage account information for members and former members as well as contact information for former members resulting from membership and governance activities.
5. Responses to member survey(s) conducted by Licking Valley RECC to identify needs or improve service.
6. Additional information about a member or a member's property, appliances and activities obtained through services offered by Licking Valley RECC or its affiliates (such as home improvements).

LICKING VALLEY RURAL ELECTRIC COOPERATIVE CORPORATION

KENTUCKY 56 MORGAN

BOARD OF DIRECTORS POLICIES AND PROCEDURES MANUAL

Policy Number 235

Effective Date: 04/21/2016

SUBJECT: PRIVACY POLICY

Page 02 of 05

B. Purposes for Collection; Access and Correction

1. Licking Valley RECC collects and maintains information about members for purposes that are suitable to its operations and management. Information is collected only through lawful and fair means and for appropriate purposes.
2. Licking Valley RECC is committed to maintaining accurate, complete, timely, relevant and appropriate information about members as necessary for the purpose for which the information is to be used. Licking Valley RECC generally permits its members to access and seek correction of records about themselves that are maintained and used by Licking Valley RECC to provide service, for billing, and to manage capital accounts. Any requests for, or disputes relating to, access, correction or other matters should be directed to:

Licking Valley RECC Cooperative Member Services
PO Box 605

West Liberty, Ky. 41472

606-743-3179 or 1-800-709-6700; or www.lvrecc.com

3. Licking Valley RECC may provide usage data to members who have access to electric usage data through an interface, such as a website (smarthub) or app.

C. How Licking Valley RECC Collects Member Information

1. When members create an account and interact with Licking Valley RECC regarding their account, utility service or participation in Licking Valley RECC programs.
2. When members use electricity service and metering systems, including smart meters.
3. When members interact with Licking Valley RECC through its website.
4. When Licking Valley RECC interacts with third parties, such as credit or collection agencies.

LICKING VALLEY RURAL ELECTRIC COOPERATIVE CORPORATION

KENTUCKY 56 MORGAN

BOARD OF DIRECTORS POLICIES AND PROCEDURES MANUAL

Policy Number 235

Effective Date: 04/21/2016

SUBJECT: PRIVACY POLICY

Page 03 of 05

D. Use and Retention of Member Information by Licking Valley RECC

1. Licking Valley RECC uses information about members in defined and responsible ways in order to manage, provide and improve its products, services and operations.
2. Data about members' electric usage may be compiled in aggregate form and such data may be used by Licking Valley RECC to improve system operations, efficiency and overall customer service.
3. Licking Valley RECC retains member information, including energy usage data, in such amounts and for such periods of time as required by law or regulation or as reasonably necessary to provide services.

E. Security

1. Licking Valley RECC maintains member information with reasonable and appropriate technical, administrative, physical and cyber safeguards to protect against loss, unauthorized access, destruction, misuse, modification, and improper disclosure of member information. Members are warned, however, that no system can ever be fully protected against every possible hazard.
2. Licking Valley RECC requires its employees, affiliates and contractors who have access to member information to comply with this privacy and confidentiality policy.
3. Member information that members may access through Licking Valley RECC's online account system is protected using cyber security protocols designed to prevent unauthorized third parties from accessing such information.

F. Disclosure to Third Parties

1. Licking Valley RECC does not share member information (e.g. a member's electric usage data and information that can reasonably be used to identify an individual) with a third party, except at the member's request, with the member's consent, or as described below. Members who wish to authorize Licking Valley RECC to disclose their information to a third party may do so by contacting Licking Valley RECC as described under G.1.

LICKING VALLEY RURAL ELECTRIC COOPERATIVE CORPORATION

KENTUCKY 56 MORGAN

BOARD OF DIRECTORS POLICIES AND PROCEDURES MANUAL

Policy Number 235

Effective Date: 04/21/2016

SUBJECT: PRIVACY POLICY

Page 04 of 05

2. Information may be disclosed to affiliates or contractors hired by Licking Valley RECC to assist in carrying out operations, such as service, maintenance, billing and management functions including legal, audit and collection services. Information may also be shared with other utilities under shared service agreements or to meet operational requirements. Information will only be disclosed to such persons to the extent necessary to render the services, and only to those who agree to maintain the confidentiality and security of the information.
3. Licking Valley RECC may disclose to and share information with commercial and consumer credit reporting agencies for credit-related and/or collection activities (e.g., the reporting of bad debts).
4. Sufficiently aggregated information may be disclosed to third parties where necessary or beneficial for Licking Valley RECC's operations (for example, to improve efficiency and overall customer service).
5. Information may be disclosed when authorized or required by law, including in response to a search warrant, subpoena or court or law enforcement order. For example, Licking Valley RECC may use and disclose records for investigations into employee misconduct or for law enforcement investigations related to its business. Disclosures may also be made when appropriate to protect Licking Valley RECC's legal rights or in situations involving an imminent threat to life or property. Licking Valley RECC will take reasonable steps to limit the scope and consequences of any of these disclosures.
6. In addition, information may be shared with affiliates and partners of Licking Valley RECC to communicate or promote services and/or information of interest to members. Members may request that their information not be shared with affiliates or partners for the offering of new products and services by contacting member services as described below. Nevertheless, Licking Valley RECC does not sell, rent, loan, exchange or otherwise release member information to non-affiliated third parties or partners for their marketing purposes, without a member's prior consent.
7. Licking Valley RECC may make information regarding third party products and services available to members through its website.

LICKING VALLEY RURAL ELECTRIC COOPERATIVE CORPORATION

KENTUCKY 56 MORGAN

BOARD OF DIRECTORS POLICIES AND PROCEDURES MANUAL

Policy Number 235

Effective Date: 04/21/2016

SUBJECT: PRIVACY POLICY

Page 05 of 05

G. How to Contact Licking Valley RECC

Questions about the policy may be directed to member services, which can be reached by phone at 606-743-3179 or 1-800-709-6700.

This Policy supersedes all prior policies with number 235.

Board Approved April 21, 2016

Secretary _____

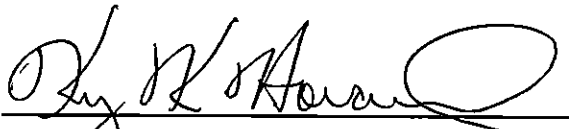
LICKING VALLEY RURAL ELECTRIC COOPERATIVE CORPORATION

PSC CASE NO. 2012-00428

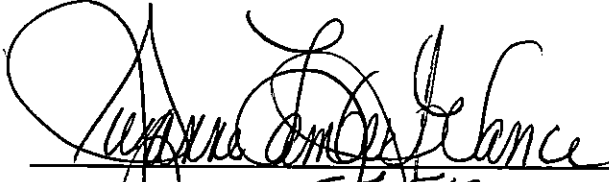
CONSIDERATION OF THE IMPLEMENTATION OF SMART GRID AND SMART
METER TECHNOLOGIES

CERTIFICATE

The undersigned, Kerry K. Howard, General Manager/CEO of Licking Valley Rural Electric Cooperative Corporation, being duly sworn, states that he has supervised the development of internal cybersecurity procedures.


Kerry K. Howard, General Manager/CEO

Subscribed and sworn before me by the Affiant, Kerry K. Howard, this 10th
day of June 2016.


Notary Public #556518
State of Kentucky at Large

My Commission Expires: 05/29/2020