Implementation10/14/2008
Revised:10/14/2009; 9/10/2019
Reviewed: 9/8/2020

POLICY: #1230– Identity Theft Prevention Policy

SCOPE OF POLICY: Board of Directors, Employees, Customers

RESPONSIBILITY: Board of Directors, General Manager

I. Policy

It shall be the policy of ERPPD (ERPPD) to take reasonable steps to identify, detect, and prevent the theft of its customers' personal information. ERPPD hereby adopts the following policy pursuant to 16 C.F.R. § 681.2 *et seq* for: (1) identifying and detecting Red Flags of identity theft; (2) responding to Red Flags of identity theft; and (3) preventing and mitigating identity theft.

Under federal law and regulations, ERPPD is required to adopt an Identity Theft Prevention Red Flag policy pursuant to the federal regulations at 16 C.F.R. § 681.2 *et seq.*

II. Procedure

A. Definitions

The term ‘‘identifying information’’ means any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including name, Social Security Number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number, or address.

The term ‘‘Identity Theft’’ means a fraud committed or attempted using the identifying information of another person without authority.

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

The terms “customer” or “customers” for purposes of this policy include all customers of ERPPD.

B. Identifications of accounts subject to Red Flag Policy

ERPPD maintains accounts for its customers that allow the customers to pay for service after it has been rendered. ERPPD does not offer banking or financial services. ERPPD maintains as a part of its customer accounts utility deposits when required for service. This account is covered by this Red Flag policy.

C. Identification of potential Red Flags

1. **Risk Factors**. In identifying potential Red Flags associated with the accounts that ERPPD maintains, ERPPD's Board of Directors and management have considered the following Identity Theft risk factors:

(a) Types of Covered Accounts. ERPPD is a rural electric distribution system serving rural Nebraska, providing its customers with electric utility service. ERPPD's service area is rural and turnover in customers is low, as is the number of address change requests received from customers. Customer accounts can consist of two different components:

(i) Payments for Utility Services Rendered. Payments from customers for services rendered are due within thirty (30) days of billing. ERPPD does not regularly provide credit to its customers beyond this revolving, monthly account for utility service. Such service is rendered at a fixed physical location known to ERPPD. As a result, there is a low risk of misuse of identifying information to perpetrate fraud on ERPPD for utility services rendered. However, identifying information maintained by ERPPD could be used to perpetrate Identity Theft and defraud other businesses if the information was wrongfully altered or disclosed.

(ii) Utility Deposits. For some customers, utility deposits may be required. These amounts are held under the terms and conditions of District's policies and may eventually be refunded to the customer. There is some risk that a customer who is a victim of Identity Theft could have the customer's utility deposit refunded to an identity thief. Additionally, identifying information maintained by ERPPD could be used to perpetrate Identity Theft and defraud other businesses in if the information was wrongfully altered or disclosed.

(b) Methods for Opening Accounts. ERPPD requires customers who wish to receive utility service provide the following information: (1) name and date of birth of adult household customers on the account; (2) address

location where service shall be provided; (3) contact and billing information; and (4) Social Security Number or Tax Identification Number.

(c) Methods for Accessing Accounts. ERPPD allows customers to access information related to their accounts using the following methods:

(i) in person at ERPPD's offices with certain identifying information matching that of the account;
(ii) over the telephone after providing ERPPD's Customer Service Representative with certain identifying information matching that of the account;.
(iii) by written request with certain identifying information matching that of the account;
(iv) via the billing portal on Elkhorn Rural Public Power's website or through the app, both with unique login and password set up by the customer;
(v) through email with certain identifying information matching that of the account.

(d) Previous Experience with Identity Theft. ERPPD is not aware of any security breach of, or unauthorized access to, its systems that are used to store customers' identifying information. ERPPD believes that part of the reason for this historical absence of Identity Theft of its customers information is due to (1) the limited services and credit provided to its customers, both of which are tied to an immovable physical location; (2) the small size of most customers utility deposits; (3) the relatively small size of the population it serves; (4) the relatively low rate of change in customers; and (5) the ERPPD's policies for securing customers' personal information.

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

(a) Alerts, Notifications, and Warnings. Alerts, notifications, or other warnings received from consumer reporting agencies or service providers, such as fraud detection services can be Red Flags for Identity Theft. Such alerts, notifications and warnings include:

(i) A fraud or active duty alert is included in a consumer report.
(ii) A consumer reporting agency provides a notice of credit freeze in response to a request for a consumer report.
(iii) A consumer reporting agency provides a notice of address discrepancy.
(iv) A consumer report indicates a pattern of activity that is inconsistent with the history and usual pattern of activity of an applicant or customer, such as:
(1) A recent and significant increase in the volume of inquiries;
(2) An unusual number of recently established credit relationships;
(3) A material change in the use of credit, especially with respect to recently established credit relationships; or
(4) An account that was closed for cause or identified for abuse of account privileges.

Required Response to Accounts: In the event a consumer report indicates an information discrepancy, it shall be the policy of ERPPD to report any such information to management for further review and verification of the potential customer's information, including verifying identification in person at ERPPD's offices. It shall further be the policy of ERPPD to train its Customer Service Representatives to look for unusual activity when reviewing customer accounts for service. Should there be unusually high inquiries on a particular account, Customer Service Representatives shall report such activity to supervisors for further review and inquiry.

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

(i) Documents provided for identification that appear to have been altered or forged.
(ii) The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.
(iii) Other information on the identification is not consistent with information provided by the person opening a new account or customer presenting the identification.
(iv) Other information on the identification is not consistent with readily accessible information that is on file with ERPPD, such as a customer application card.
(v) A document appears to have been altered or forged or gives the appearance of having been destroyed and reassembled.

Required Response to Suspicious Documents. Customer Service Representatives and other personnel of ERPPD shall report to management when it appears that account documents have been altered or forged when compared to other documents in a customer's file. It shall also be brought to a supervisor's attention immediately if any customer presents an invalid identification, or identification that appears forged for the purpose of obtaining access to account information.

(c) Suspicious Personal Identifying Information. The presentation of suspicious personal identifying information, such as a suspicious address change, can be a Red Flag for Identity Theft. Presentation of suspicious personal identifying information occurs when:

(i) Personal identifying information provided is inconsistent when compared against external information sources used by ERPPD. For example:
(1) The address does not match any address in the consumer report; or
(2) The Social Security Number has not been issued or is listed on the Social Security Administration's Death Master File.

(ii) Personal identifying information provided by the customer is not consistent with other personal identifying information provided by the customer. For example, there is a lack of correlation between the Social Security Number range and date of birth.

(iii) Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by ERPPD, for example:

(1) The address on an application is the same as the address provided on a fraudulent application; or

(2) The phone number on an application is the same as the number provided on a fraudulent application.

(iv) Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by ERPPD. For example:

(1) The address on an application is fictitious, a mail drop, or a prison; or

(2) The phone number is invalid or is associated with a pager or answering service.

(v) The Social Security Number provided is the same as that submitted by other persons opening an account or other customers.

(vi) The address or telephone number provided is the same as or similar to the account number or telephone number submitted by an unusually large number of other persons opening accounts or other customers.

(vii) The person opening the covered account, or the customer fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete.

(viii) Personal identifying information provided is not consistent with personal identifying information that is on file with ERPPD.

Required Response to Personal ID Information. ERPPD shall provide customers access to their account information in person at the ERPPD's offices only after verifying the customer's identity. Access to customer account information via telephone or internet shall require the customer to verify his or her identity using information that would only

be known to the customer as reflected in the customer's account. Customer Service Representatives shall be trained to make note in a customer's file when there is a lack of correlation between information provided by a customer and information contained in a file for the purposes of gaining access to account information. ERPPD is not to provide account information without first clearing any discrepancies in the information provided.

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

(i) Shortly following the notice of a change of address for a customer account, ERPPD receives a request for the addition of authorized users on the account.
(ii) Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's covered account.
(iii) ERPPD is notified that the customer is not receiving paper account statements.
(iv) ERPPD is notified of unauthorized charges or transactions in connection with the customer's account.
(v) A customer requests a utility deposit refund check be sent to a new address without requesting a service disconnection or change in service location.
(vi) A customer requests that a utility deposit refund check be made payable to a person other than the customer.
(vii) A customer requests that ERPPD provide the customer with personal identifying information from the ERPPD's records.

Required Response to Suspicious Activity. Customer Service Representatives shall be trained to note unusual use of accounts, or suspicious activities related to accounts and verify the identity of customers in such circumstances. It shall further be the policy of ERPPD to not provide identifying information to customers, either verbally or in writing, even when customers are asking for their own information.

Customer Service Representatives shall immediately notify management, who will conduct further reasonable inquiry, when a customer requests such information. It shall be the policy of ERPPD to train its Customer Service Representatives to look for unusual activity when reviewing customer accounts for service. Customer Service Representatives shall also notify a supervisor when there are an unusually high number of inquiries on an account, coupled with a lack of correlation in the information provided by the customer. For requests for ERPPD customer lists for use in ERPPD elections, ERPPD shall take steps to ensure that the requested information is only disclosed in accordance with its Customer Information Request policy.

(f) Notices. Notices of potential identity theft are also serious Red Flags, including:

(i) Notice from customers, law enforcement authorities, or other persons indicating that a customer has been a victim of Identity Theft;
(ii) Notice to ERPPD that a customer has provided information to someone fraudulently claiming to represent ERPPD;
(iii) Notice to ERPPD that a fraudulent website that appears similar to ERPPD's website is being used to solicit customer personal identifying information;
(iv) The ERPPD's mail servers are receiving returned e-mails that ERPPD did not send, indicating that is customer may have received a fraudulent e-mail soliciting customer personal identifying information.

Response to Notice of Red Flag: Upon notice from a customer, law enforcement authority, or other persons that one of its customers may be a victim of Identity Theft, ERPPD shall contact the customer directly in order to determine what steps may be necessary to protect any customer information in the possession of ERPPD. Such steps may include, but not be limited to, setting up a new account for the customer with additional identifying information that may be identified only by the customer in order to protect the

integrity of the customer's account, or notifying customers and the media of an on-going attempt to perpetrate a fraud on the customers of ERPPD.

D. Detecting Red Flags

1. It shall be the policy of ERPPD to obtain identifying information about, and verify the identity of, a person opening an account. ERPPD will obtain the customer's name, date of birth, address for service location, and Social Security Number or Tax Identification Number to open a new account. It shall be the policy of ERPPD to not provide identifying information to customers, either verbally or in writing, even when a customer is asking for their own information.

2. It shall be the policy of ERPPD to authenticate and monitor transactions and verify the validity of change of address requests, in the case of existing accounts.

E. Preventing and Mitigating Identity Theft

1. If ERPPD discovers that any of its customers have become victims of Identity Theft or its system containing the identifying information has been breached, ERPPD shall take appropriate steps to mitigate the impacts of such Identity Theft. These steps may include, but are not limited to:

   (a) Monitoring an account for evidence of Identity Theft;
   (b) Contacting the customer;
   (c) Changing any passwords, security codes, or other security devices that permit access to an account;
   (d) Reopening an account with a new account number;
   (e) Closing an existing account;
   (f) Not attempting to collect on an account;
   (g) Notifying the customer in compliance with federal law and *Neb. Rev. Stat.* §87-803;
   (h) Notifying law enforcement or the Nebraska Attorney General if required by *Neb. Rev. Stat.* §87-801 *et. seq*

(i) Putting a stop payment on any outstanding utility deposit refund checks;
(j) Putting a hold on any utility deposit refund checks; or
(k) Determining that no response is warranted under the particular circumstances.

2. ERPPD has a business relationship with third party contractors for maintaining the customer billing system, archiving customer data, etc. Under this business relationship, the third-party contractors have access to customer identifying information covered under this Policy. The General Manager shall ensure that the third party contractor's work for ERPPD is consistent with this policy by (a) amending the contract to incorporate these requirements; or (b) by determining that the third party contractors have reasonable alternative safeguards that provide the same or a greater level of protection for customer information as provided by ERPPD.

F. Policy Updates and Administration

1. ERPPD shall consider updates at least annually to determine whether it has experienced any Identity Theft of its customers' accounts, whether changes in the methods of Identity Theft require updates to this policy, and whether changes are necessary to detect, prevent, and mitigate Identity Theft. ERPPD management will continue to monitor changes in methods of Identity Theft and re-evaluate this policy in light of those changes. Management believes that review of such changes on no more than an annual basis is necessary.

2. Administration of this Policy shall be as follows:

(a) The Board of Directors has adopted this policy and will have ultimate authority over this policy, but the policy shall be managed by General Manager of ERPPD. The General Manager shall have authority to delegate oversight and compliance to other individuals at the management level. The General Manager shall be responsible for reviewing staff and management reports regarding compliance with this policy.

(b) Potential changes to the policy shall be reviewed at least annually by ERPPD management. Material changes to the policy that may be needed prior to the meeting described herein shall be brought to the General Manager's attention and reviewed by management and the Board of Directors if deemed necessary by the General Manager.

(c) Reports:

(i) Management personnel assigned responsibility under this policy or by delegation from the General Manager shall prepare a report, at least annually, regarding the implementation and progress of ERPPD's policy for review by the General Manager. The General Manager may, at his or her discretion, bring any issues related to the policy to the attention of the Board of Directors for review.

(ii) The above-described report prepared by management personnel designated with supervising the policy shall include a discussion of: the progress of implementing and the effectiveness of the policy; ongoing risk level of Identity Theft of customer information; potential changes to the policy and other operation practices of ERPPD to further the goal of protecting customer's personal information; and, identification and discussion of instances of Identity Theft of ERPPD's customers.

(iii) The General Manager shall keep records, such as board of director meeting minutes, of meetings regarding this policy showing the dates and topics discussed. The General Manager shall also cause to be maintained a file with copies of the five (5) most recent annual reports prepared under the policy.