

RESOLUTION NO. 0913

IDENTITY THEFT PREVENTION PROGRAM

WHEREAS, the Eugene Water & Electric Board (EWEB) recognizes the importance of establishing a Identity Theft Prevention Program (Program) and procedures for the purposes of detecting, preventing and mitigating possible identity theft risks to customers in connection with opening an account or any existing account(s); or to the safety and soundness of EWEB from identity theft.

WHEREAS, the Eugene Water & Electric Board has the responsibility to protect personal information within customer data and to create a Program that meets the standards established by the Federal Trade Commission (FTC) by May 1, 2009; and which contains the following elements:

- (i) Identifying red flags for covered account(s) to be incorporated in the Program;
- (ii) Detecting red flags incorporated into the Program;
- (iii) Responding appropriately to any red flags that are detected to prevent and mitigate identity theft; and
- (iv) Ensuring the Program is updated periodically to reflect changes in risks to customers and EWEB from identity theft.

THEREFORE, BE IT RESOLVED that the Eugene Water & Electric Board approves the initial Identity Theft Prevention Program and hereby directs the General Manger to develop an appropriate committee and/or a designated employee of senior management in the oversight, development, implementation and administration of the Program.

Dated this 21st day of April 2009.

THE CITY OF EUGENE, OREGON
Acting by and through the
Eugene Water & Electric Board

President

I, KRISTA K. HINCE, the duly appointed, qualified and acting Assistant Secretary of the Eugene Water & Electric Board do hereby certify that the above is a true and exact copy of the Resolution adopted by the Board at its regular meeting of April 21, 2009.

Assistant Secretary



Eugene Water & Electric Board

Rely on us.

EWEB IDENTITY THEFT PREVENTION PROGRAM

Document Owner:

Authoring Department: Corporate Services Division

Resides with:

Document Number:

Revision Number: 0

Approved/Revision Date:

On-Line Location: R:\Share\

File Name: EWEB Identity Theft Prevention Program

EWEB Privacy Committee

Approval

Signature

Date

Randy Berggren

General Manger &
Chief Compliance Officer
& General Manager

Jim Origliosso

Corporate Services Division Director
& Privacy Committee Officer

1.0 PURPOSE

This document creates an Identity Theft Prevention Program that utilizes guidelines set forth in the Fair and Accurate Credit Transactions Act (2003) in order to safeguard personal customer information within the workplace in order to identify Red Flags that will alert our employees when new or existing accounts are opened using false information, protect against the establishment of false accounts, establish methods to ensure existing accounts were not opened using false information and designate measures to respond to such events.

2.0 BACKGROUND:

2.1 2003: Passage of the federal Fair Accurate Credit Transactions Act (FACT Act).

- **Requires** each financial institution or creditor (utilities included) to develop and implement a written Identity Theft Prevention Program to detect, prevent and mitigate identity theft in connection with the opening of covered a covered account or any existing covered account, 6CFR 681.2(d).
- **Issues** guidelines to assist entities in the formation and maintenance of a Program that satisfies the requirements of the rules.
- **Sets** forth responsibilities for the Board of Directors.

2.2 2007: Passage of the Oregon Consumer Theft Protection Act (SB 583)

- **Requires** notification be provided to individuals whose personal information was subject to a security breach, if a security breach occurs.
- **Restricts** the display or disclosure of the social security number, drivers license number, passport number, financial account number and other identification numbers upon any materials not requested by the consumer or part of the documentation of a transaction or service requested by the consumer that are mailed to a consumer; printed on a card used to access services; publicly posted or displayed; unless redacted (altered so only the last four digits appear on the data).
- **Requires** the development, implementation and maintenance of reasonable safeguards to protect the security, confidentiality and integrity of personal information including the disposal of such data.
- **Acknowledges** compliance with this law if an entity complies with a state or federal law that provides greater protection to personal information than the administrative, technical and physical guidelines which are similar to the FACT Act.
- **Establishes** an operative date of January 1, 2008.

2.3 2007: Final Rule for FACT Act Issued November 9, 2007.

- **Sets** mandatory compliance date for this rule by November 1, 2008; however, on October 22, 2008, the Federal Trade Commission issued an Enforcement Policy statement that delays enforcement of the Red Flags rule until May 1, 2009.

3.0 SCOPE

This Program applies to management and all personnel of EWEB. This Program supplements and doesn't replace EWEB Policies and Procedures relating to the integrity of customer information for covered accounts.

4.0 RESPONSIBILITY

EWEB has a responsibility to protect personal information within customer data and to create a Program that meets standards established by the Federal Trade Commission (FTC) by May 1, 2009. The Program elements include: (i) identifying red flags for covered accounts to be incorporated in the Program; (ii) detecting red flags incorporated into the Program; (iii) responding appropriately to any red flags that are detected to prevent and mitigate identity theft; and (iv) ensuring the Program is updated periodically to reflect changes in risks to customers and EWEB from identity theft. The Privacy Committee is charged with the continuing management and development of the Program.

5.0 TERMS AND ABBREVIATIONS

5.1 CIS:

Customer Information System

5.2 CS:

Customer Service

5.3 Company:

Company refers to the Eugene Water & Electric Board (EWEB).

5.4 Identity Theft:

The term "identity theft" means a fraud committed or attempted using the identifying information of another person without authority. "Identifying information" means any name or number that may be used alone or in conjunction with any other information to identify a specific person. Fraudulent activity may include using another consumer's name, social security number or other identifying information of a consumer without the consumer's authority, for the purpose of establishing an account with EWEB or transacting financial business with EWEB.

5.5 Nationwide consumer reporting agency (NCRA).

An NCRA is an agency that compiles and maintains files on consumers on a nationwide basis and regularly engages in the practice of assembling or evaluating

and maintaining the following two pieces of information about consumers residing nationwide for the purpose of furnishing consumer reports to third parties bearing on a consumer's credit worthiness, credit standing or credit capacity, 15 U.S.C. 1681a(p).

- Public record information:
- Credit account information from persons who furnish that information regularly and in the ordinary course of business.

5.6 Notice of address discrepancy:

A notice sent to a user by an NCRA that informs the user of a substantial difference between the address for the consumer that the user provided to request the consumer report and the address(es) in the NRCA's file for the consumer 16 CFR 681.1(b).

5.7 Red Flag:

Red Flag means a pattern or specific activity that indicates the possible existence of identity theft.

6.0 ROLES AND RESPONSIBILITIES

6.1. The Privacy Committee is responsible for:

- (a) Appointing a Chief Privacy Officer.
- (b) Performing a "Needs Assessment" and identifying EWEB's strengths and areas of improvements in opening new customer accounts and monitoring existing customer accounts.
- (c) Reviewing and updating policies and procedures.
- (d) Conducting Program evaluation.
- (e) Insuring employee training takes place.
- (f) Periodic walk-through to assess compliance and look for opportunities to enhance prevention, identification and mitigation of red flags.
- (g) Leading quarterly review of significant events such as incidents or patterns or near misses.
- (h) Preparing reports to the General Manager describing program effectiveness, including information on:
 - a. Events experienced and established outcomes since last report.
 - b. Precautions or steps used in the utility Program.
 - c. Requesting Board of Commissioners approval for proposed changes.

- d. Establishing a relationship with local law officials.

6.2 Duties of EWEB when an NCRA provides EWEB with a Notice of Address Discrepancy.

(a) Requirement to form a reasonable belief: EWEB must develop and implement reasonable policies and procedures designed to enable it to form a reasonable belief that the consumer report relates to the consumer whose report was requested, when the user receives a notice of address discrepancy in connection with a new or existing account, 16CFR 681.1(c).

EWEB may form a reasonable belief by comparing information in the consumer report with information it:

- a. Has obtained and used to verify the consumer's identity as required in EWEB Customer Services Policies and Procedures, All Utilities, Section B, Application for Service;
- b. Maintains its own records;
- c. Obtains from a third party; or
- d. Verifies directly with the customer.

6.3 Requirement to furnish a consumer's address to NCRA:

(a) EWEB must develop and implement reasonable policies and procedures for furnishing an address for the customer that the user has reasonably confirmed is accurate to the NCRA from whom it received the notice of address discrepancy when EWEB:

(b) Can form a reasonable belief that the consumer report relates to the consumer whose report was requested:

- a. Establishes a continuing relationship with the consumer (i.e. in connection with a new account); and
- b. Regularly and in the ordinary course of business furnishes information to the NCRA that provided the notice of address discrepancy.

(c) EWEB may reasonably confirm an address is accurate by:

- a. Verifying the address with the consumer about whom it has requested a report;
- b. Reviewing EWEB records to verify the address of the consumer;
- c. Verifying the address through third-party sources; or,
- d. Using other reasonable means.

7.0 RESPONDING TO RED FLAGS

7.1 Chart of Red Flags Detection & Next Steps.

- a. EWEB has identified the following Red Flags as useful in detecting potential fraudulent activity. The Red Flags identified below are not intended to be all-inclusive and other suspicious activity may be investigated and responded to, as necessary.
- b. If a Red Flag identified in the first column is detected, the second column, Next Step, outlines the process for addressing the Red Flag.

Flag	Next Step
Consumer report indicates fraud or active duty alert.	Follow directions on consumer report to reasonably confirm identity before opening an account.
Credit freeze.	Follow directions on consumer report to reasonably confirm identity before opening an account.
Identification documents appear altered or forged.	Advise customer the form of identification is unacceptable; document CIS records of the Red Flag; DO NOT OPEN ACCT; and require customer to visit office in order to confirm identification.
Photo/physical description does not match applicant.	Advise customer the form of identification is unacceptable; document CIS records and DO NOT OPEN ACCT and require customer to visit office.
Other information on identification is inconsistent information given from applicant.	Advise customer the form of identification is unacceptable; document CIS records and DO NOT OPEN ACCT and require customer to visit office.
Information in utility files is inconsistent with information provided. Example – signatures do not match on signature card.	Advise customer the form of identification is unacceptable; document CIS records and DO NOT OPEN ACCT and require customer to visit office.
Identification is inconsistent with external source such as: - Address v. Address on Consumer Report	As appropriate, place a conference call to SS office or applicable external source with customer participating in the teleconference.

Flag	Next Step
<ul style="list-style-type: none"> - 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>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>Customer is required to come into office to resolve.</p> <p>CIS only accepts one customer number per account, but allows multiple locations for same customer.</p> <p>CIS provides automatic warning for further investigation (Credit Bureau/SS Office).</p>
<p>Applicant fails to provide all personal ID requested.</p>	<p>Do not open account</p>
<p>Personal ID is inconsistent with utility records.</p>	<p>Require verification via SS office or acceptable government issued, photo-ID</p>

Flag	Next Step
Payments are made in a manner associated with fraud. For example, deposit or initial payment is made and no payments are made thereafter.	CIS delinquency process flags account(s).
Existing account with a stable history shows irregularities.	Conduct validity tests, re-read, meter(s) and perform field visit as appropriate.
An account with low activity unexpectedly jumps to high consumption. Ex: 1000 kwh to 2801 kwh.	Investigate with field visit to verify meter readings.
Mail sent to customer is repeatedly returned.	Attempt customer contact via contact information in CIS.
Customer notifies utility that they are not receiving their bill.	Verify address info, refer to US PO
The utility is notified of unauthorized charges or transactions in connection with a customer's account.	Investigate with telephone contact, field visit, follow automated delinquency process
Utility is notified by law officials or others, that it has opened a fraudulent account for a person engaged in identity theft.	Deliver door hanger asking for valid customer to sign and return. If no response is received in designate time, service is disconnected.

8.0 BREACH

- 8.1. In the event a breach of security has occurred, procedures covered in CS & P&P, All Utilities, Section 3, under FRAUD will be followed.
- 8.2 Breach of security will be coordinated with the Human Resources Department and related policies regarding staff breach of security.
- 8.3 In the event of a breach of security of EWEB data that includes a customer's personal information, EWEB shall give notice of the breach of security following discovery of such breach of security in accordance with ORS 646A.604 to any customer whose personal information was included in the information breach.

9.0 RECORD DISPOSAL

9.1 Procedures for Maintaining, Shredding & Destroying Documents.

- (a) **Customer Service:** EWEB maintains locking shred bins in available work areas. Subject to the Minimum Record Board Retention Requirement Policy, staff is required to shred all documents containing customer information after it is no longer required for business purposes or retained in accordance with the state or federal law.
- (b) **Collecting and Protecting Documents and Data until the Time of Destruction:** EWEB follows the Minimum Record Board Retention Requirement Policy.
- (c) **Documentation of Record Destruction:** EWEB follows the Minimum Record Board Retention Requirement Policy.

10.0 TRAINING & SCREENING

10.1 Identified Managers and Supervisors who have “a need to know” will be responsible for training staff on the identity theft program.

11.0 REPORTS OF SUSPECTED IDENTITY THEFT

11.1 Process:

- (a) In the event that EWEB receives notification of a suspected identity theft from a customer:
 - a. CS staff will request the account-holder notify EWEB in writing by submitting an appropriate, notarized form.

- b. CS staff will make a copy of account-holder's ID and attach to the submitted form together with the police report. These documents will be submitted to the Privacy Officer.
- d. CS staff will close or block the affected account(s) and open new account(s) if appropriate.
- e. CS staff will place notification of the reported of the reported identity theft on the CIS system.
- f. CIS documentation will be used as the notification method for CS.

11.2 Victims Record Request:

- (a) EWEB will provide victims of identity theft all related business transaction records within 30 days at no cost to the victim.

11.3 Release of Information:

- (b) EWEB will provide identity theft related business transactions records to law enforcement agencies in accordance with Customer Service Policies and Procedures, All Utilities, Section D, 1 – 6, Release of Information Concerning Customers.

12.0 REFERENCE DOCUMENTS

12.1 Identity Theft Prevention Programs in American Utilities – Guidelines for Compliance with Red Flags.

12.2 FACT Act (2003) – 72 Fed. Register 63718, Sections 114 & 315

ATTACHMENT

EWEB'S Privacy Committee
Red Flags Identity Theft Program

