

CITY OF BELLFLOWER

RESOLUTION NO. 08-63

A RESOLUTION OF THE CITY COUNCIL OF THE CITY OF BELLFLOWER ADOPTING AN IDENTITY THEFT PREVENTION PROGRAM FOR THE MUNICIPAL WATER SYSTEM

WHEREAS, the Federal Trade Commission has adopted regulations that require "creditors" holding consumer or other "covered accounts" (which are defined to mean any account where customer payment information is collected in order to bill for services rendered) to develop and implement by May 1, 2009, an identity theft prevention program that complies with those regulations; and

WHEREAS, because the City provides retail water service to its customers, it is a "creditor" under the applicable Federal Trade Commission regulations and must, therefore, comply with those regulations by adopting and implementing an identity theft prevention program; and

WHEREAS, the City Council desires to take action to comply with the applicable Federal Trade Commission regulations by adopting an identity theft prevention program; and

WHEREAS, the City contracts with Bellflower-Somerset Mutual Water Company for the operation of the Municipal Water System.

NOW, THEREFORE, BE IT RESOLVED BY THE CITY COUNCIL OF THE CITY OF BELLFLOWER AS FOLLOWS:

SECTION 1. The City Council finds that pursuant to 16 CFR § 681.2, the Bellflower-Somerset Mutual Water Company Identity Theft Protection Program:

- a. Identifies red flag warning signs or activities that will alert the Operator to potential identity theft and establishes policies and procedures that respond to red flags in a manner that will prevent and mitigate identity theft with respect to covered accounts; and
- b. Establishes policies and procedures relating to address discrepancies between information provided by a consumer and information provided by a consumer credit company.

SECTION 2. The City Council of the City of Bellflower hereby adopts Bellflower-Somerset Mutual Water Company Identity Theft Protection Program (Exhibit "A") as the City of Bellflower Municipal Water System Identity Theft Protection Program.

SECTION 3. Any changes to the Program as they relate to the Municipal Water System will be approved by the City Council.

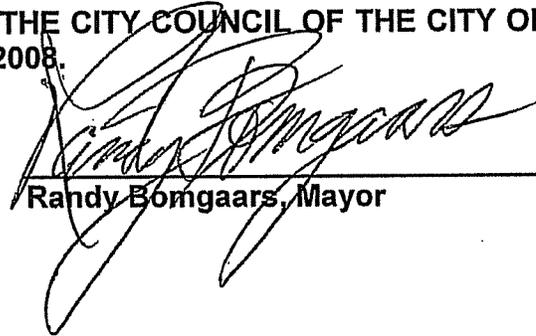
SECTION 4. On or before April 10 of each year the Operator will submit a written report to the City Manager addressing the effectiveness of the program, documenting significant incidents involving identity theft and related responses, providing updates related to external service providers, and including recommendations for material changes to the

program. The City Manager will review the Operator's report and make appropriate recommendations to the City Council.

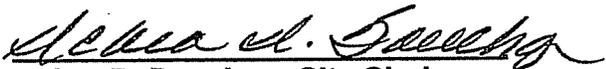
SECTION 5. The Mayor, or presiding officer, is hereby authorized to affix his signature to this Resolution signifying its adoption by the City Council of the City of Bellflower, and the City Clerk, or her duly appointed deputy, is directed to attest thereto.

PASSED, APPROVED, AND ADOPTED BY THE CITY COUNCIL OF THE CITY OF BELLFLOWER ON THIS 27th DAY OF OCTOBER 2008.

Attest:



Randy Bomgaars, Mayor



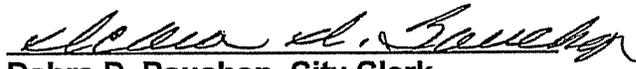
Debra D. Bauchop, City Clerk

STATE OF CALIFORNIA)
COUNTY OF LOS ANGELES)SS
CITY OF BELLFLOWER)

I, **Debra D. Bauchop**, City Clerk of the City of Bellflower, California, do hereby certify under penalty of perjury that the foregoing Resolution No. 08-63 was duly passed, approved, and adopted by the City Council of the City of Bellflower at its Regular Meeting of October 27, 2008, by the following vote to wit:

AYES: Council Members – Larsen, Smith, Dunton, and Mayor Bomgaars
ABSENT: Council Member - King

Dated: October 28, 2008


Debra D. Bauchop, City Clerk
City of Bellflower, California

(SEAL)

Exhibit A

**CITY OF BELLFLOWER
RESOLUTION NO. 08-63**

BELLFLOWER-SOMERSET MUTUAL WATER COMPANY

Identity Theft Prevention Program

This program is in response to and in compliance with the
Fair and Accurate Credit Transaction (FACT) Act of 2003

and

The final rules and guidelines for the FACT Act issued by the
Federal Trade Commission and federal bank regulatory agencies
in November 2007

Adopted October XX, 2008 – Resolution # 10-20-08

Identity Theft Prevention Program

Purpose

This document was created in order to comply with regulations issued by the Federal Trade Commission (FTC) as part of the implementation of the Fair and Accurate Credit Transaction (FACT) Act of 2003. The FACT Act requires that financial institutions and creditors implement written programs which provide for detection of and response to specific activities ("red flags") that could be related to identity theft. These programs must be in place by November 1, 2008.

The FTC regulations require that the program must:

1. Identify relevant red flags and incorporate them into the program
2. Identify ways to detect red flags
3. Include appropriate responses to red flags
4. Address new and changing risks through periodic program updates
5. Include a process for administration and oversight of the program

Program Details

Relevant Red Flags

Red flags are warning signs or activities that alert a creditor to potential identity theft. The guidelines published by the FTC include 26 examples of red flags which fall into the five categories below:

- Alerts, notifications, or other warnings received from consumer reporting agencies or service providers
- Presentation of suspicious documents
- Presentation of suspicious personal identifying information
- Unusual use of, or other suspicious activity related to, a covered account
- Notice from customers, victims of identity theft, or law enforcement authorities

After reviewing the FTC guidelines and examples, Bellflower-Somerset Mutual Water Company (the "Company") determined that the following red flags are applicable to its customer accounts. These red flags, and the appropriate responses, are the focus of this program.

- A consumer credit reporting agency reports the following in response to a credit check request:
 - Fraud or active duty alert
 - Credit freeze
 - The Social Security Number (SSN) is invalid or belongs to a deceased person
 - The age or gender on the credit report is clearly inconsistent with information provided by the customer
- Suspicious Documents and Activities
 - Documents provided for identification appear to have been altered or forged.
 - The photograph on the identification is not consistent with the physical appearance of the customer.
 - Other information on the identification is not consistent with information provided by the customer.
 - The SSN provided by the customer belongs to another customer in the Company's records.
 - The customer does not provide required identification documents when attempting to establish an account with the Company or make a payment.
 - A customer refuses to provide proof of identity when discussing a Company account.
 - A person other than the account holder or co-applicant requests information or asks to make changes to an established account.
 - An employee requests access to information a customer account unrelated to any business purpose of the Company.

- A customer notifies the Company of any of the following activities:
 - Billing statements are not being received
 - Unauthorized changes to a customer's account
 - Unauthorized charges on a customer's account
 - Fraudulent activity on the customer's bank account or any credit card that is used to pay water charges to the Company.
- The Company is notified by a customer, a victim of identity theft, or a member of law enforcement that an account at the Company has been opened for a person engaged in identity theft.

Detecting and Responding to Red Flags

Red flags will be detected as Company employees interact with customers and the City's credit reporting agency. An employee will be alerted to these red flags during the following processes:

- Establishing a new customer account: When establishing a new account, a customer is asked to provide a SSN so the Company can run a credit check. Reports from the credit reporting agency may contain red flags.

Response: Do not establish the new account. Ask the customer to appear in person and provide a government-issued photo identification. A deposit may also be required in order to establish service.

- Reviewing customer identification in order to establish an account or process a payment: A Company employee may be presented with documents that appear altered or inconsistent with the information provided by the customer.

Response: Do not establish the account or accept payment until the customer's identity has been confirmed.

- Answering customer inquiries on the phone, via email, and at the counter: Someone other than the account holder or co-applicant may ask for information about a customer's account or may ask to make changes to the information on an account. A customer may also refuse to verify their identity when asking about an account.

Response: Inform the customer that the account holder or the co-applicant must give permission for them to receive information about the subject account. Do not make changes to or provide any information about the account, with one exception: if the service on the account has been interrupted for non-payment, the Company may provide the payment amount needed for reconnection of service.

- Receiving notification that there is unauthorized activity associated with a customer's account: Customers may call to alert the Company about fraudulent activity related to their account and/or any bank account or credit card used to make payments on the account.

Response: Verify the customer's identity, and notify the General Manager immediately. Take the appropriate actions to correct the errors on the account, which may include:

- Issuing a service order to connect or disconnect services
 - Assisting the customer with deactivation of their payment method, such as on-line bill paying or automatic debiting, if applicable
 - Updating personal information on the customer's account
 - Updating the mailing address on the customer's account
 - Updating account notes to document the fraudulent activity
 - Adding a password to the account
 - Notifying and working with law enforcement officials
- Receiving notification that a customer account has been established for a person engaged in identity theft.

Response: These issues should be escalated to the General Manager immediately. The claim will be investigated, and appropriate action will be taken to resolve the issue as quickly as possible.

Additional procedures that help to protect against identity theft include:

- Access to the Company's billing system and customer records is limited to a "need-to-know" and "need to use" basis, and only certain job classifications have access to the system.
- At such time as the Company provides on-line or telephone access to customer accounts, customers will be required to enroll using their customer account number and service address, and will also be required to create a unique user identification and password.
- The Company will ensure that its billing system and customer records are protected with appropriate technology to protect against external hackers accessing the system and those records.

Administration and Oversight of the Program

Company staff will annually report on the effectiveness of the program, document significant incidents involving identity theft and related responses, provide updates related to any external service providers, and include recommendations for any necessary material changes to the program.

The program will be reviewed at least annually and updated as needed based on the following events:

- Experience with identity theft
- Changes to the types of accounts and/or programs the Company offers
- Implementation of new systems and/or new vendor contracts

Specific roles with respect to the program are as follows:

- The Company's Board of Directors shall approve and adopt the initial program.
- The Office Manager will oversee the daily activities related to identity theft detection and prevention, and ensure that all pertinent Company staff are trained to detect and respond to red flags.
- The Office Manager will also report to the General Manager on an annual basis on the effectiveness of the program and shall include in that report any incidents of identity theft the Company experienced since the prior report and any recommendations for improvements or changes to the program.
- The General Manager will provide ongoing oversight to ensure that the program is effective and will review the Office Manager's annual report and approve recommended changes to the program, both annually and on an as-needed basis.