# CITY OF LONG BEACH

DEPARTMENT OF FINANCIAL MANAGEMENT

333 West Ocean Blvd • Long Beach, California 90802


**C-5**

June 23, 2009

HONORABLE MAYOR AND CITY COUNCIL
City of Long Beach
California

RECOMMENDATION:

Adopt a Resolution approving the existing Identity Theft Prevention Program in compliance with the Fair and Accurate Credit Transaction (FACT) Act. (Citywide)

DISCUSSION

In accordance with the FACT Act adopted by the federal government, the Federal Trade Commission (FTC) has set "Red Flag" rules requiring that every creditor establish a written program providing for the detection of Red Flags that could be related to identity theft. Any private or public entity that extends credit to customers by first providing goods or services and then billing for them at a later date is subject to these requirements.

As a municipal service provider, the City is considered a creditor since it provides various services such as gas, water and ambulance transport services and bills for these services after they have been rendered.

Along with all other municipal utility providers in the nation, the City is required to formally adopt its Identity Theft Prevention Program (Program) by August 1, 2009. The Program complies with FTC requirements and provides security for our utility customers.

The Program sets forth in writing the identity protection practices that the City has followed for many years, namely:

1. Identifying relevant patterns, practices and specific activities (referred to in the program as "Red Flags") that signal possible identity theft relating to information maintained in the City's customer accounts, both those currently existing and those accounts to be established in the future.

2. Detecting "Red Flags."

3. Responding promptly and appropriately to detected "Red Flags" to prevent or mitigate identity theft relating to the City's customer account information.

4. Ensuring that the program is updated periodically to reflect any necessary changes.

This matter was reviewed by Deputy City Attorney Richard Anthony on May 19, 2009 and Budget and Performance Management Bureau Manager David Wodynski on May 20, 2009.

TIMING CONSIDERATION

City Council action on this matter is requested on June 23, 2009 in order to adopt the Program prior to the August 1, 2009 deadline.

FISCAL IMPACT

The "Red Flag" program has no significant fiscal impact since its policies and procedures do not differ from the City's existing utility billing policies or practices.

SUGGESTED ACTION:

Approve recommendation.

Respectfully submitted,

LORI ANN FARRELL
DIRECTOR OF FINANCIAL MANAGEMENT/CFO

LAF:PH
K:\Exec\Council Letters\Commercial Services\Misc\06-23-09 ccl - Red Flag - FACT Act.doc

ATTACHMENT

APPROVED:

PATRICK H. WEST
CITY MANAGER

RESOLUTION NO.

A RESOLUTION OF THE CITY COUNCIL OF THE CITY OF LONG BEACH ADOPTING A WRITTEN IDENTITY THEFT PREVENTION PROGRAM AS REQUIRED BY THE FAIR AND ACCURATE CREDIT TRANSACTION ACT.

WHEREAS, the Federal Government has adopted the Fair and Accurate Credit Transaction (FACT) Act which is meant, among other things, to reduce identity theft; and

WHEREAS, exercising authority given it by the FACT Act, the Federal Trade Commission (FTC) has adopted rules requiring all creditors to establish and formally adopt a written program providing for the detection of certain indicators that could be related to identity theft; and

WHEREAS, the City of Long Beach qualifies as a creditor for purposes of the FTC rules and is required to establish and adopt such a written program;

NOW, THEREFORE, the City Council of the City of Long Beach resolves as follows:

Section 1. The City hereby adopts and approves the Identity Theft Prevention Program attached hereto as Exhibit "A".

Section 2. This resolution shall take effect immediately upon its adoption by the City Council, and the City Clerk shall certify the vote adopting this resolution.

//

//

//

//

//

//

OFFICE OF THE CITY ATTORNEY
ROBERT E. SHANNON, City Attorney
333 West Ocean Boulevard, 11th Floor
Long Beach, CA 90802-4664

I hereby certify that the foregoing resolution was adopted by the City Council of the City of Long Beach at its meeting of _____, 20___ by the following vote:

Ayes: Councilmembers: _____

_____

_____

_____

Noes: Councilmembers: _____

_____

Absent: Councilmembers: _____

_____

_____

City Clerk

OFFICE OF THE CITY ATTORNEY
ROBERT E. SHANNON, City Attorney
333 West Ocean Boulevard, 11th Floor
Long Beach, CA 90802-4664

# EXHIBIT “A”

**Subject:** **Identity Theft Prevention Program (Red Flags Program)**

**Effective: 05-01-2009**



## 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 that 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 August 1, 2009.

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 examples of red flags which fall into the following categories:

- 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, the Commercial Services Bureau determined that the following red flags are applicable to utility accounts. These red flags, and the appropriate responses, are the focus of this program.

1. Suspicious Documents and Activities
   i. Documents provided for identification appear to have been altered or forged.
   ii. The photograph on the identification is not consistent with the physical appearance of the customer.
   iii. Other information on the identification is not consistent with information provided by the customer.
   iv. The customer does not provide required identification documents when attempting to re-establish a utility account or make a payment; this does not apply to accounts turned off for non-payment.
   v. A person other than the account holder or co-applicant requests information or asks to make changes to an established utility account.
   vi. An employee requests access to the billing system or information about a utility account, and the request is inconsistent with the employee's role in the City.

2. A customer notifies the Commercial Services Bureau of any of the following activities:
   i. Utility statements are not being received several months in a row.
   ii. Unauthorized changes to a utility account.
   iii. Fraudulent activity on the customer's bank account or a credit card that is used to pay utility charges.

3. The Commercial Services Bureau is notified by a customer, a victim of identity theft, or a member of law enforcement that a utility account has been opened for a person engaged in identity theft.

Detecting and Responding to Red Flags

Red flags will be detected as utility billing employees interact with customers. An employee will be alerted to these red flags during the following processes:

1. Establishing a new utility account: When establishing a new account, a customer is asked to provide a name, social security number and service address. The utility billing employee may be presented with information that appears to be inconsistent.

**Response:** Do not establish the utility account until the customer's identity has been confirmed.

2. Reviewing customer identification in order to process an automated payment or enroll the customer electronically in the automatic EasyPay program: The utility billing employee may be presented with documents that appear altered or inconsistent with the information provided by the customer.

**Response:** Do not accept payment electronically until the customer's identity has been confirmed.

3. Answering customer inquiries on the phone, via email, and at the counter: Someone who can't properly identify the account holder may ask for information about a utility account (including utility web accounts) or may ask to make changes to the information on an account. A customer may also refuse to verify his/her identity when asking about an account.

**Response:** Inform the customer that proper ID must be provided in order to receive information about the utility 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 utility billing employee may provide the payment amount needed for reconnection of service.

4. Processing requests from City of Long Beach employees: Employees may submit requests for information from the billing system that is inconsistent with the role that they play at the City.

**Response:** All requests for direct access to the billing system are approved by the Utility Customer Services Officer; any requests that have not received appropriate approval, will be rejected by the Technology Services Department. All other requests for information from the billing system should be reviewed to ensure that they do not violate any part of the policy. Requests that are inconsistent with the policy will be denied.

5. Receiving notification that there is unauthorized activity associated with a utility account: Customers may call to alert the City about fraudulent activity related to their utility account and/or the bank account or credit card used to make payments on the account.

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

i. Issuing a service order to connect or disconnect services.
ii. Assisting the customer with deactivation of their payment method (EasyPay).
iii. Updating personal information on the utility account.
iv. Updating the mailing address on the utility account.
v. Updating account notes to document the fraudulent activity.
vi. Notifying and working with law enforcement officials.

6. Receiving notification that a utility account has been established for a person engaged in identity theft.

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

7. Preventing and mitigating identity theft.

**Response:** Commercial Services Bureau staff will take the following steps with respect to its internal operating procedures to protect customer identifying information by:

i. Continue to monitor an account for evidence of identity theft.
ii. Contact the customer.
iii. Change any passwords or other security devices that permit access to accounts.
iv. Close an existing account.
v. Establish an account with a new number.
vi. Notify the Bureau Manager to determine which appropriate steps to take.
vii. Notify law enforcement; or
viii. Determine that no response is warranted under these particular circumstances.

7. Protect Customer Identification Information by:

**Response:** Take appropriate action to keep customer information protected by:

i. Ensure that the CSB website is secure or provide clear notice that the website is not secure.
ii. Ensure complete and secure destruction of paper documents and computer files containing customer information.
iii. Ensure the office computers are password protected and that computer screens lock after a set period of time;
iv. Keep offices clear of papers containing customer information;
v. Request only the last four digits of social security numbers (if any).
vi. Require and keep customer information that is necessary for utility purposes.
vii. Ensure all stored documents/media containing customer secure information are in locked drawer/area;
viii. Ensure all computer files containing customer secure information are in password-protected folders.

Additional procedures that help to protect against identity theft include:

1. Utility billing system access is based on the role of the user. Only certain job classifications have access to the entire system.
2. Customers may access limited information about their utility account online. In order to access information online, customers must use their utility account number and the last four digits of their Social Security number or predetermined PIN number.

## Administration and Oversight of Program

Commercial Services Supervisors with the assistance of Technology Services staff are required to prepare an annual report which addresses the effectiveness of the program, documents significant incidents involving identity theft and related responses, provides updates related to external service providers, and includes recommendations for material changes to the program.

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

1. Experience with identity theft
2. Changes to the types of accounts and/or programs offered
3. Implementation of new systems and/or new vendor contracts.

Specific roles are as follows:

The Commercial Services Supervisor will submit an annual report to the Utility Services Officer and the Technology Services Officer. The Commercial Services Supervisor will also oversee the daily activities related to identity theft detection and prevention, and ensure that all members of the Commercial Services Bureau are trained to detect and respond to Red Flags.

The Commercial Services Bureau Manager will provide ongoing oversight to ensure that the program is effective.

The Commercial Services Officer will review the annual report and approve recommended changes to the program, both annually and on an as-needed basis.

The Commercial Services Bureau Manager must approve the initial program.