



## AGENDA REPORT

**Meeting Date:** April 7, 2009  
**Item Number:** F-6  
**To:** Honorable Mayor & City Council  
**From:** Dr. Scott Miller, CFO / Director of Administrative Services  
**Subject:** RESOLUTION OF THE COUNCIL OF THE CITY OF BEVERLY HILLS  
APPROVING THE CUSTOMER IDENTIFICATION AND CREDIT  
INFORMATION PROTECTION PROGRAM IN COMPLIANCE WITH  
THE FAIR AND ACCURATE CREDIT TRANSACTIONS ACT OF 2003

**Attachments:** 1) Resolution  
2) Identify Theft Prevention Program

---

### **RECOMMENDATION**

Staff recommends that the City Council adopt a resolution approving a formal policy on Identity Theft Protection as required by the Federal Trade Commission for the Fair and Accurate Credit Transactions Act (FACT Act) of 2003.

### **INTRODUCTION**

The Fair and Accurate Credit Transaction Act requires entities which affect consumer credit to evaluate and possibly create a formal program to detect, prevent and mitigate identity theft before May 1, 2009.

### **DISCUSSION**

In accordance with the FACT Act rules, the consumer identification and credit information protection program must:

- 1) Identify red flags, defined as patterns, practices or specific activities that indicate the possible existence of identity theft, for covered accounts and incorporate those red flags into the program;
- 2) Detect red flags that have been incorporated into the program;
- 3) Respond appropriately to any red flags that are detected to prevent and mitigate identity theft;

- 4) Ensure the program is updated periodically, to reflect changes in identity theft risk to customers or the creditor;
- 5) Provide for administration of the program.

To date, there have been no known attempts to compromise the City's information systems or any unauthorized attempts to access customer information. In the event there is any indication of physical or electronic threat to customer credit or identity security, the Administrative Services Department will work with the Information Technology Department, the City Attorney's Office and the Beverly Hills Police Department as appropriate to eliminate the threat.

The identity theft prevention program is included as Attachment 1.

**FISCAL IMPACT**

The net impact from this program on the Administrative Services Department operating budget is not expected to be of any significance as there is no known capital costs associated with implementing or updating the program.



---

Dr. Scott G. Miller / CFO  
Finance Approval

# **Attachment 1**

Resolution

RESOLUTION NO. 09-R-\_\_\_\_\_

RESOLUTION OF THE COUNCIL OF THE CITY OF  
BEVERLY HILLS APPROVING THE CUSTOMER  
IDENTIFICATION AND CREDIT INFORMATION  
PROTECTION PROGRAM IN COMPLIANCE WITH THE  
FAIR AND ACCURATE CREDIT TRANSACTIONS  
ACT OF 2003

The City Council of the City of Beverly Hills does resolve as follows:

A. The Federal Trade Commission ("FTC") rule under the Fair and Accurate Credit Transactions Act ("FACT Act") requires entities which affect consumer credit to evaluate and possibly create a formal program to detect, prevent, and mitigate identity theft before May 1, 2009; and

B. A public utility is considered to offer or maintain accounts covered under the FACT Act; and

C. The City of Beverly Hills ("City") has conducted a risk assessment to determine whether the accounts it maintains are subject to a reasonably foreseeable risk of identity theft, including a review of (1) the methods used to open accounts, (2) the methods of accessing accounts, and (3) previous experiences with identity theft; and

D. City has identified relevant "red flags" defined as patterns, practices or specific activities that indicate the possible existence of identity theft; and

E. City has reviewed its processes for opening, maintaining and accessing covered accounts; and

F. There have been no known cases of attempts at unauthorized access to customer identity and account information; and

G. City has identified new processes either for immediate implementation or for implementation in conjunction with the customer information system scheduled to be online in 2009.

NOW, THEREFORE, BE IT RESOLVED by the City of Beverly Hills City Council as follows:

Section 1. The Council hereby approves the "Procedures for Customer Credit Security" Program, attached hereto as Exhibit A.

Section 2. The City Clerk shall certify to the adoption of this resolution and shall cause this resolution and his certification to be entered in the Book of Resolutions of the Council of this City.

Adopted:

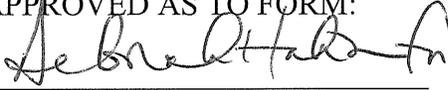
\_\_\_\_\_  
NANCY KRASNE  
Mayor of the City of Beverly Hills

ATTEST:

\_\_\_\_\_  
(SEAL)  
BYRON POPE  
City Clerk

[Signatures continue]

APPROVED AS TO FORM:



LAURENCE S. WIENER  
City Attorney

APPROVED AS TO CONTENT:



SCOTT G. MILLER  
Director of Administrative Services/Chief  
Financial Officer



DAVID D. GUSTAVSON  
Director of Public Works & Transportation

## **Attachment 2**

### Identity Theft Prevention Program



# **Identity Theft Prevention Program**

**City of Beverly Hills**  
**Administrative Services Department**  
*Updated March 10, 2009*

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.

# 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 May 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 26 examples of red flags which fall into the five categories below:

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

After reviewing the FTC guidelines and examples, the Finance Division determined that the following red flags are applicable to utility 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 City's computer system.
  - The customer does not provide required identification documents when attempting to establish a utility account.
  - A customer refuses to provide proof of identity when discussing an established utility account.
  - A person other than the account holder or co-applicant requests information or asks to make changes to an established utility account.
  - An employee requests access to the Utility Billing system or information about a utility account, and the request is inconsistent with the employee's need or ability to perform their official duties.
  - A customer notifies the Utility Billing Services Division of any of the following activities:
    - Utility statements are not being received.
    - Unauthorized changes to a utility account.
    - Fraudulent activity on the customer's bank account or credit card that is used to pay utility charges.
  - The Utility Billing Services Division is notified by a customer, a victim of identity theft, or a member of law enforcement that a utilities 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 Services Division employees interact with customers and the City's credit reporting agency. An employee will be alerted to these red flags during the following processes:

*Situation: Reviewing customer identification in order to establish an account:* The CSRs may be presented with documents that appear altered or inconsistent with the information provided by the customer.

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

*Situation: 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 utility 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 utility account. Do not make changes to or provide any information about the account, with one exception: if a person or agency makes payment on behalf of customer account.

*Situation: Processing requests from City of Beverly Hills employees:* Employees may submit requests for information in the Utility Billing system that is inconsistent with the employee's need or ability to perform their official duties

**Response:** All requests for direct access to the Utility Billing system must be approved by the CFO (or designee).

*Situation: 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 Customer Service Supervisor 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.*
- *Updating personal information on the utility account.*
- *Updating the mailing address on the utility account.*
- *Updating account notes to document the fraudulent activity.*
- *Notifying and working with law enforcement officials.*

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

**Response:** These issues should be escalated to the Customer Service Supervisor 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:**

- The Utility Billing system access is based on the role of the user. Only certain job classifications have access to the entire system.
- The Finance Department will destroy paper receipts generated during credit card payment processing not less than 60 days after receipt is made.
- The Finance Department will ensure that service providers that receive and process utility billing information have programs in place to detect and prevent identity theft.

## **Administration and Oversight of the Program**

The CFO (or designee) is 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:

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

Specific roles are as follows:

- The Assistant Director of Administrative Services – Finance (or designee) will submit an annual report to the CFO.
- The Administrative Services Director/CFO will review the annual report and approve recommended changes to the program, both annually and on an as-needed basis.
- The CFO (or designee) will oversee the daily activities related to identity theft detection and prevention, and ensure that all members of the Finance Division staff are trained to detect and respond to red flags.
- The CFO (or designee) will provide ongoing oversight to ensure that the program is effective.
- The City Council must approve the initial program.