Item #9-6

City of Carson City
Agenda Report

Date Submitted: April 24, 2009

Agenda Date Requested: May 7, 2009
Time Requested: Consent

To: Board of Supervisors

From: Jennifer Schultz, Human Resources Director, representing the Policy and Procedure Task Force

Subject Title: Action to approve the Identity Theft Prevention Policy.

Staff Summary: To ensure compliance with the Federal Trade Commissions' Fair and Accurate Transaction Act (FACTA) of 2003, the City's Policies and Procedure Task Force drafted a policy addressing identity theft prevention.

Type of Action Requested: (check one)

(____) Resolution
(__X_) Formal Action/Motion
(____) Ordinance
(____) Other (Specify)

Does This Action Require A Business Impact Statement: (___) Yes (_X_) No

Recommended Board Action: I move to approve the Identity Theft Prevention Policy.

Explanation for Recommended Board Action: Approval of this Board Action ensures Carson City is compliant with FACTA.

Applicable Statue, Code, Policy, Rule or Regulation: n/a

Fiscal Impact: Minimal cost associated with staff training and program record keeping.

Explanation of Impact: The Board of Supervisors is requested to approve this policy.

Funding Source: General Fund

Alternatives: Approval or denial.

Supporting Material: Policy

Prepared By: Jennifer Schultz, H.R. Director

Reviewed By:

(Department Head) Date: 4/28/09

(City Manager) Date: 4/28/09

(District Attorney) Date: 4-28-09

Michele Brownlee Date: 4/28/09

(Finance Director)

Board Action Taken:

Motion: _____ 1) _____ Aye/Nay

2) _____ _____

_____

_____

_____

_____

_____

(Vote Recorded By)

POLICY AND PROCEDURE

Subject:		Index:	
Identity Theft Prevention		**Number:**	
Effective Date: May 1, 2009	**Supersedes:** n/a	**Pages:** 4	**Approved by:**

1.0 PURPOSE:
To assist in detecting, preventing and mitigating identity theft.

2.0 ORGANIZATIONS AFFECTED:
All departments organized as part of the Executive Branch as identified in or created pursuant to Article 3 of the Carson City Charter except those specifically exempted.

3.0 REFERENCES:
Fair and Accurate Transaction Act of 2003

4.0 POLICY:
This policy is established in accordance with the rules adopted by the Federal Trade Commission, to implement the Fair and Accurate Transaction Act of 2003 (FACTA). Carson City, as a credit account provider that allows its customers to pay for certain City services after the services have been received, is required to adopt an Identity Theft Prevention Program to protect customers.

5.0 DEFINITIONS:

5.1 Covered account: any account the City offers or maintains primarily for personal, family, or household purposes, that involves multiple payments or transactions; and

Any other account the City offers or maintains for which there is a reasonable foreseeable risk to customers or to the safety and soundness of the City from identity theft.

5.2 Identifying information: any name or number that may be used alone, or in conjunction with any other information, to identify a specific person, including: name, address, telephone number, social security number, date of birth, government-issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number, unique electronic identification number, computer's Internet Protocol address, or routing number.

6.0 PROCEDURES:

6.1 The following are identified as red flags, which are potential indicators of fraud. Any time a red flag, or a situation closely resembling a red flag, is apparent, it should be investigated for verification.

6.1.1 Suspicious Documents

6.1.1.1 Documents provided for identification that appear to have been altered or forged.

6.1.1.2 The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.

6.1.1.3 Other information on the identification is not consistent with information provided by the person opening a new covered account or customer presenting the identification.

6.1.1.4 Other information on the identification is not consistent with readily accessible information that is on file with the City, such as a signature card or recent check.

6.1.1.5 An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

6.1.2 Suspicious Personal Identifying Information

6.1.2.1 Personal identifying information provided is inconsistent when compared against external information sources used by the City. For example:

6.1.2.1.1 The social security number (SSN) has not been issued, or the number is listed on the Social Security Administrator's Death Master File.

6.1.2.2 Personal identifying information provided by the customer is not consistent with other personal identifying information provided by the customer.

6.1.2.3 Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the City.

6.1.2.4 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.

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

6.1.2.6 Personal identifying information provided is not consistent with personal identifying information that is on file with the City.

6.1.2.7 The person opening the covered account or the customer cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report in the event the City elects to include as part of the account application the requirement for the

applicant to provide the answer to a challenge question to be used to verify the identity of the customer when asking for the information.

6.2 Unusual Use of, or Suspicious Activity Related to, the Covered Account

6.2.1 A new account is used in a manner commonly associated with known fraud patterns. For example:

6.2.1.1 The customer fails to make the first payment or makes an initial payment, but not subsequent payments or the City is notified that the customer is not receiving their paper account statements.

7.0 Notice from Customers, Victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts held by the creditor.

7.1 The City is notified by a customer, a victim of identify theft, a law enforcement authority, or any other person that the City has opened a fraudulent account for a person engaged in identity theft.

8.0 Incidents of identity theft the City has experienced

8.1 The customer's behavior, or the information provided by the customer, is consistent or similar to that of other customers the City has experienced as having been relating to incidents of identity theft.

8.2 Other patterns of behavior the City experiences from time-to-time that have been used in identity theft.

9.0 Procedures to Detect Red Flags

9.1 The City Treasurer, or the Treasurer's designee, shall serve as the Program Administrator.

9.2 The Program Administrator shall have the following duties:

9.2.1 Developing, implementing and updating this Program.

9.2.2 Administration of this Program.

9.2.3 Ensuring the City staff are appropriately trained.

9.2.4 Reviewing the staff reports regarding the detection of red flags and the steps for preventing and mitigating identity theft.

9.2.5 Determining the steps or prevention and mitigation should be taken in particular circumstances.

9.2.6 Considering period changes to the Program.

9.3 Staff Training and Reports

9.3.1 City staff responsible for implementing this Program shall be trained either by or under the direction of the Program Administrator in the detection of red flags and the responsive steps to be taken when a red flag is detected.

9.3.2 Staff should prepare a report at least annually for the Program Administrator, including but not limited to the following:

9.3.2.1 An evaluation of the effectiveness of the Program with respect to operating accounts.

9.3.2.2 An evaluation of existing covered accounts.

9.3.2.3 An evaluation of service provider arrangements.

9.3.2.4 Significant incidents involving identity theft and response.

9.3.2.5 Recommendations for changes to the Program.

9.4 Service Provider Arrangements

9.4.1 In the event the City engages a service provider to perform an activity in connection with one or more accounts, the City will take the following steps to ensure the service provider performs its activity in accordance with reasonable policies designed to detect, prevent, and mitigate risk of identity theft.

9.4.1.1 Require, by contract, the service provider to have such policies and procedures in place; and

9.4.1.2 Require, by contract, the service provider review this Program and report any red flags to the Program Administrator.

9.5 Periodic Updating of the Program

9.5.1 This Program will be reviewed by the Program Administrator at least annually to determine if the Program needs to be amended to reflect changes in risks to customers and to determine the soundness of the Program to protect City covered accounts from identity theft. The review shall include at least the following:

9.5.1.1 Additions or modifications to the red flags, based on the following:

9.5.1.1.1 The City's experience with identity theft;

9.5.1.1.2 New information regarding red flags presented from other sources, including but not limited to, credit reporting agencies and law enforcement.

9.5.1.2 Changes in methods of identity theft.

9.5.1.3 Changes in methods to detect, prevent and mitigate identity theft.

9.5.1.4 Changes in business arrangements.

9.5.1.5 Changes in types of accounts offered.

9.5.1.6 Changes in the City's business arrangements with other entities.

END OF SECTION