CITY OF OAKWOOD
ADMINISTRATIVE POLICIES AND PROCEDURES

POLICY NO. 14
SUBJECT: Identity Theft "Red Flags" Mitigation Program
DATE: June 1, 2009
RECOMMENDED BY: _____
CINDY STAFFORD, FINANCE DIRECTOR

CONCURRED BY: _____
DALMA GRANDJEAN, CITY ATTORNEY

APPROVED BY: _____
NORBERT S. KLOPSCH, CITY MANAGER

POLICY: This policy is required by the Federal Fair and Accurate Credit Transaction Act of 2003 which was an amendment to the Fair Credit Reporting Act.

PURPOSE: To establish an Identity Theft Mitigation Program designed to detect, prevent and mitigate identity theft in connection with the opening of a covered account or an existing covered account and to provide for continued administration of the Program in compliance with Part 681 of Title 16 of the Code of Federal Regulations implementing Sections 114 and 315 of the Fair and Accurate Credit Transactions Act (FACTA) of 2003.

DEFINITIONS

Identify theft means fraud committed or attempted using the identifying information of another person without authority.

A **covered account** means:

1. An account that a financial institution or creditor offers or maintains, primarily for personal, family, or household purposes that involves or is designed to permit multiple payments or transactions. Covered accounts include credit card accounts, cell phone accounts, utility accounts, payroll accounts, checking accounts and savings accounts; and

2. Any other account that the financial institution or creditor offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the financial institution or creditor from identity theft, including financial, operational, compliance, reputation or litigation risks.

A **red flag** means a pattern, practice or specific activity that indicates the possible existence of identity theft.

THE PROGRAM

The city of Oakwood Finance Department establishes an Identity Theft Mitigation Program to detect, prevent and mitigate identity theft. The Program shall include reasonable policies and procedures to:

1. Identify relevant red flags for covered accounts it offers or maintains 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; and

4. Ensure the Program is updated periodically to reflect changes in risks to customers and to the safety and soundness of the creditor from identity theft.

The program shall, as appropriate, incorporate existing policies and procedures that control reasonably foreseeable risks.

Administration of Program

1. The Director of Finance shall be responsible for the development, implementation, oversight and continued administration of the Program.

2. The Program shall include staff training, as necessary, to effectively implement the Program; and

3. The Program shall exercise appropriate and effective oversight of service provider arrangements.

Identification of Relevant Red Flags

1. The Program shall include relevant red flags from the following categories as appropriate:

    a. Alerts, notifications, or other warnings received from consumer reporting agencies or service providers, such as fraud detection services;

    b. The presentation of suspicious documents;

    c. The presentation of suspicious personal identifying information;

    d. The unusual use of, or other suspicious activity related to, a covered account; and

e. Notices from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts.

2. The Program shall consider the following risk factors in identifying relevant red flags for covered accounts as appropriate:

   a. The types of covered accounts offered or maintained;

   b. The methods provided to open covered accounts;

   c. The methods provided to access covered accounts; and

   d. Its previous experience with identity theft.

3. The Program shall incorporate relevant red flags from sources such as:

   a. Incidents of identity theft previously experienced;

   b. Methods of identity theft that reflect changes in risk; and

   c. Applicable supervisory guidance.

Detection of Red Flags

The Program shall address the detection of red flags in connection with the opening of covered accounts and existing covered accounts, such as by:

1. Obtaining identifying information about, and verifying the identity of, a person opening a covered account; and

2. Authenticating customers, monitoring transactions, and verifying the validity of change of address requests in the case of existing covered accounts.

Response

The Program shall provide for appropriate responses to detected red flags to prevent and mitigate identity theft. The response shall be commensurate with the degree of risk posed. Appropriate responses may include:

1. Monitor a covered account for evidence of identity theft;

2. Contact the customer;

3. Change any passwords, security codes or other security devices that permit access to a covered account;

4. Reopen a covered account with a new account number;

5. Not open a new covered account;

6. Close an existing covered account;

7. Notify law enforcement; or

8. Determine no response is warranted under the particular circumstances.

Updating the Program

The Program shall be updated periodically to reflect changes in risks to customers or to the safety and soundness of the organization from identity theft based on factors such as:

1. The experiences of the organization with identity theft;

2. Changes in methods of identity theft;

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

4. Changes in the types of accounts that the organization offers or maintains;

5. Changes in the business arrangements of the organization, including mergers, acquisitions, alliances, joint ventures and service provider arrangements.

Oversight of the Program

1. Oversight of the Program shall include:

    a. Assignment of specific responsibility for implementation of the Program;

    b. Review of reports prepared by staff regarding compliance;

    c. Periodic review and evaluation of the effectiveness of the Program; and

    d. Approval of material changes to the Program as necessary to address changing risks of identity theft.

Oversight of Service Provider Arrangements

The city of Oakwood Finance Department shall take steps to ensure that the activity of a service provider is conducted in accordance with reasonable policies and procedures designed to detect, prevent and mitigate the risk of identity theft whenever the organization engages a service provider to perform an activity in connection with one or more covered accounts.

Use of Credit Reporting Agencies and Duties Regarding Discrepancies

The city of Oakwood Finance Department shall develop policies and procedures designed to enable the organization to form a reasonable belief that a credit report relates to the consumer for whom it was requested if the organization receives a notice of address discrepancy from a nationwide consumer reporting agency indicating the address given by the consumer differs from the address contained in the consumer report.

The city of Oakwood Finance Department may reasonably confirm that an address is accurate by any of the following means:

1. Verification of the address with the consumer;
2. Review of the utility's records;
3. Verification of the address through third-party sources; or
4. Other reasonable means.

If an accurate address is confirmed, the organization (utility) shall furnish the consumer's address to the nationwide consumer reporting agency from which it received the notice of address discrepancy if:

1. The organization establishes a continuing relationship with the consumer; and
2. The organization, regularly and in the ordinary course of business, furnishes information to the consumer reporting agency.