


CITY OF GRAND RAPIDS

ADMINISTRATIVE POLICY

NUMBER: 09-01	DATE: May 15, 2009
REVISIONS:	
ISSUED BY: City Manager	SIGNED: 

SUBJECT: IDENTITY THEFT PREVENTION PROGRAM

PURPOSE: To outline an Identity Theft Prevention Program (“Program”) designed to detect, prevent and mitigate identity theft in connection with covered accounts originated and/or serviced by the City of Grand Rapids (“City”) 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.

POLICY:

1. Definitions:

- a. **Identify theft** - fraud committed or attempted using identifying information of another person without authority.
- b. **Identifying information** - any name or number that may be used, alone or in conjunction with other information, to identify a specific person, including: name, address, telephone number, social security number, date of birth, government issued driver’s licenses of identification number, alien registration number, government passport number, employer or taxpayer identification number, unique electronic identification number, computer’s Internet Protocol address or routing code.
- c. **Covered account** - an account the City offers or maintains, primarily for personal, family, or household purposes, that permits multiple payments or transactions. Covered accounts include mortgage loans, utility accounts, and any other account the City offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the City from identity theft, including financial, operational, compliance, reputation or litigation risks.
- d. **Red flag** - a pattern, practice or specific activity that indicates the possible existence of identity theft.

2. Administration of the Program:

- a. The City Manager or designee shall be responsible for the development, implementation, oversight and continued administration of the Program.
- b. The Program shall train staff, as necessary, to effectively implement the Program; and
- c. The Program shall exercise appropriate and effective oversight of service provider arrangements.

3. Identification of Red Flags:

Red flags from the following categories will be used to detect fraudulent activity related to City accounts:

- 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; and
- d. Notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with loan accounts.

4. Detection of Red Flags:

In order to detect red flags related to City accounts, staff shall:

- a. Require customers to present government-issued identification information to open an account. Types of necessary information include:
 - 1) Name
 - 2) Date of Birth
 - 3) Social Security Number
 - 4) Address
 - 5) Phone Number
 - 6) Photo Identification
- b. Verify personal identification information using records on file or through a third-party source such as a consumer reporting agency.
- c. Independently contact the customer (in the case of phone or internet set up of accounts).
- d. When fielding a request to access and/or modify an existing account (such as a change of billing address), verify identity of customer by requesting specific pieces of personal identifying information (identification with the new billing address and/or documentation proving shift of financial liability)
- e. If new banking information is provided for electronic payments of accounts, cross-check ownership of the new bank account with the customer name on the customer account by contacting the appropriate financial institution.
- f. For online or automated phone system access of account, require the establishment of security questions during the initial set-up of the account.

5. Response to Detection of Red Flags:

Responses to detection of red flags shall be commensurate with the degree of risk posed. Appropriate responses may include:

- a. Monitoring an account for evidence of identity theft;
- b. Contacting the customer for additional documentation;
- c. Notifying immediate supervisor;

- d. Reopening an account with a new account number;
- e. Not opening a new account;
- f. Closing an existing account;
- g. Notifying law enforcement; or
- h. Determining no response is warranted under the particular circumstances.

6. 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:

- a. The experiences of the City with identity theft;
- b. Changes in methods of identity theft;
- c. Changes in methods of detection, prevention and mitigation of identity theft;
- d. Changes in the types of accounts that the City offers or maintains;
- e. Changes in the business arrangements of the organization, such as joint ventures and service provider arrangements.

7. Oversight of the Program:

- a. Oversight of the Program shall include:
 - 1) Assignment of specific responsibility for implementation of the Program;
 - 2) Review of reports prepared by staff regarding compliance; and
 - 3) Approval of material changes to the Program as necessary to address changing risk of identity theft.
- b. Reports shall be prepared under the following guidelines:
 - 1) Staff responsible for development, implementation and administration of the Program shall report to the City Manager or designee at least annually regarding compliance with the Program.
 - 2) Reports shall address material matters related to the Program and evaluate issues such as:
 - i. Effectiveness of policies and procedures in addressing risk of identity theft in connection with the opening of covered accounts and with respect to existing covered accounts;
 - ii. Service provider agreements;
 - iii. Significant incidents involving identity theft and management's response;
 - iv. Recommendations for material changes to the Program.

8. Oversight of Service Provider Arrangements:

Whenever the City engages a service provider to perform an activity in connection with one or more covered accounts, the City shall take steps to ensure the service provider activity is conducted in accordance with reasonable policies and procedures designed to detect, prevent and mitigate the risk of identity theft.

9. Duties Regarding Address Discrepancies:

If the City receives notice of address discrepancy from a consumer reporting agency, the City will implement the following methods to reach a reasonable belief that a credit report relates to the consumer for whom it was requested.

- a. Verification of the address with the consumer;

- b. Review of City account records;
- c. Verification of the address through third-party sources; or
- d. Other reasonable means.

10. Identity theft Prevention Program Review and Approval:

Appropriate staff has been trained on the procedures of this Identity theft Prevention Program.

This policy has been reviewed and approved by the Grand Rapids City Commission on April 14, 2009, City Commission Proceeding No.781964.