RESOLUTION NO. 10 , 2009

A RESOLUTION ADOPTING AN IDENTITY THEFT (RED FLAG) POLICY

WHEREAS, the Fair and Accurate Credit Transactions Act of 2003, an amendment to the Fair Credit Reporting Act, required rules to be promulgated regarding identity theft protection; and

WHEREAS, the Federal Trade Commission, among other organizations charged with this rule-making authority, have jointly adopted rules which become effective May 1, 2009, which require any business organization which allows deferred payments for goods or services to comply with the rules regarding identity theft protection; and

WHEREAS, the administration and the Financial Planning Committee of City Council have determined that the attached policy regarding identity theft protection, commonly referred to as the Red Flag Policy, is in the best interest of the City and should be adopted effective March 1, 2009.

NOW THEREFORE, BE IT RESOLVED by the Council of the City of Montgomery, Hamilton County, Ohio, that:

SECTION 1. The attached Identity Theft Policy (Red Flag Policy) shall be adopted by the City effective March 1, 2009. With the implementation of the policy, the administration shall take the appropriate steps to identify a Program Coordinator and to begin training of the staff to identify and secure sensitive information, and to be alert to red flags which may indicate identity theft or consumer fraud.

SECTION 2. This Resolution shall be in full force and effect from and after its passage.

PASSED: February 4, 2009

ATTEST: Susan J. Hamm
Susan J. Hamm, Clerk of Council

Gerri Harbison
Gerri Harbison, Mayor

APPROVED AS TO FORM:

Terrence M. Donnellon
Terrence M. Donnellon, Law Director

CITY OF MONTGOMERY	**Policy No:** VII-22 **Effective Date:** March, 2009 **Revision Date:**

POLICY #VII-22, IDENTITY THEFT PREVENTION PROGRAM

1. **Purpose.** The purpose of this program is to enable the City to protect employees and citizens from damages related to the loss or misuse of sensitive information; to reduce risk from identity fraud and minimize potential damage to the City from fraudulent new accounts; to help the City identify risks that signify potentially fraudulent activity within new or existing covered accounts; detect risks when they occur in covered accounts; respond to risks to determine if fraudulent activity has occurred and to take appropriate action if fraud has been attempted or committed; and to update the program periodically including reviewing the accounts that are covered and the identified risks that are a part of the program.

2. **Definitions.** For purposes of this program, the following terms shall have the following definitions:

Covered account: means an account that the City offers or maintains, primarily for personal, family, or household purposes that involves or is designed to permit multiple payments or transactions such as credit card accounts, utility accounts, and any other account that 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.

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

Program Coordinator: means Finance Director or his/her designee.

Red flag: means a pattern, practice or specific activity that indicates the possible existence of identity theft.

Sensitive Information: means the following items whether stored in electronic or printed format: Credit card information, (credit card number, expiration date, cardholder name); Tax identification numbers; Social Security numbers; Employer identification numbers; Personal information such as, date of birth, address, phone numbers, maiden name, customer number.

3. **Sensitive Information.** City personnel are to use common sense judgment in securing sensitive information. File cabinets, desk drawers, overhead cabinets, and any other storage space containing documents with sensitive information will be secured when not in use. Storage rooms containing documents with sensitive information and record retention areas will be locked at the end of each workday or when unsupervised. Desks, workstations, work areas, printers and fax machines, and common shared work areas should be cleared of all documents containing sensitive information when not in use.

4. **Red Flags.** At any time that any of the following red flags are present, City personnel are to make an appropriate investigation for verification:

(a) Alerts, notifications or warnings from a consumer reporting agency;

(b) A fraud or active duty alert included with a consumer report;

(c) A notice of credit freeze from a consumer reporting agency in response to a request for a consumer report;

(d) A notice of address discrepancy from a consumer reporting agency.

(e) Consumer reports that indicate a pattern of activity inconsistent with the history and usual pattern of activity of an applicant or customer, such as: A recent and significant increase in the volume of inquiries; An unusual number of recently established credit relationships; A material change in the use of credit, especially with respect to recently established credit relationships; or An account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor.

(f) Documents provided for identification that appear to have been altered or forged.

(g) Photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification or other information on the identification is not consistent with information provided by the person opening a new covered account or customer presenting the identification.

(h) Information on the identification is not consistent with readily accessible information that is on file with the City, such as a signature card or a recent check.

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

(j) Personal identifying information provided is inconsistent when compared against external information sources regularly used by the City.

(k) Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the City. For example, the address on an application is the same as the address provided on a fraudulent application.

(l) Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the City. For example: the address on an application is fictitious, a mail drop, or a prison; or the phone number is invalid or is associated with a pager or answering service.

(m) The social security number provided is the same as that submitted by other persons opening an account or other customers.

(n) The address or telephone number provided is the same as or similar to the address or telephone number submitted by an unusually large number of other customers or other persons opening accounts.

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

(p) Personal identifying information provided is not consistent with personal identifying information that is on file with the City.

(q) When using security questions (mother's maiden name, pet's name, etc.), 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.

(r) Shortly following the notice of a change of address for a covered account, the City receives a request for new, additional, or replacement goods or services, or for the addition of authorized users on the account.

(s) A new account is used in a manner commonly associated with known patterns of fraud patterns. For example, the customer fails to make the first payment or makes an initial payment but no subsequent payments.

(t) A covered account is used in a manner that is not consistent with established patterns of activity on the account. There is, for example nonpayment when there is no history of late or missed payments.

(u) A covered account that has been inactive for a reasonably lengthy period of time is used (taking into consideration the type of account, the expected pattern of usage and other relevant factors).

(v) Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's covered account.

(w) The City is notified that the customer is not receiving paper account statements.

(x) The City is notified of unauthorized charges or transactions in connection with a customer's covered account.

(y) The City receives 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 City.

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

5. Responding to Red Flags. Once potentially fraudulent activity is detected, (a red flag is identified) an employee must act quickly as a rapid appropriate response can protect customers and the City from damages and loss. Once potentially fraudulent activity is detected, the employee is to gather all related documentation and write a description of the situation and present this information to the Program Coordinator who will then complete additional authentication to determine the appropriate response.

6. Appropriate Responses for Suspected Fraud. An appropriate response for suspected fraudulent activity may include:

(a) Further monitoring a covered account for evidence of identity theft;

(b) Contacting the customer;

(c) Changing any passwords, security codes or other security devices that permit access to a covered account;

(d) Reopening a covered account with a new account number;

(e) Not opening a new covered account;

(f) Closing an existing covered account;

(g) Notifying law enforcement; or

(h) Determining no response is warranted under the particular circumstances.

6. Appropriate Responses for Fraudulent Actions. If a transaction is determined to be fraudulent, appropriate actions must be taken immediately. Actions may include:

(a) Canceling the transaction;

(b) Notifying and cooperating with appropriate law enforcement;

(c) Determining the extent of liability of the City; and

(e) Notifying the actual customer that fraud has been attempted.

7. Duties Regarding Address Discrepancies. In the event the City uses a consumer report and receives a notice from a consumer reporting agency of an address discrepancy, the appropriate employee shall establish that the consumer report relates to the consumer about whom the City has requested the consumer report. This may be done by: verification of the address with the consumer; review of the utility's records; verification of the address through third-party sources; or other reasonable means.

8. Updating Program. At periodic intervals as established by the administration, or as may be required to address changes in risks to customers, citizens or the City, the program will be re-evaluated to determine whether all aspects of the program are up to date and applicable in the current business environment. Periodic reviews will include an assessment of which accounts are covered by the program and whether or not additional sensitive information should be identified. As a part of the review, red flags may be revised, replaced or eliminated. Defining new red flags also may be appropriate as well as identifying action steps to take in the event that fraudulent activity is discovered to reduce damage to the City, its citizens and customers.

9. Oversight of Program. The Program Coordinator shall oversee and take steps to ensure that this Program is being followed. Oversight of this Program shall include: assignment of specific responsibility for implementation of this Program; review of reports prepared by staff regarding compliance; and approval of material changes to this Program as necessary to address changing risks of identity theft. The reports by staff shall address material matters related to the Program and evaluate issues such as: the effectiveness of the program in addressing the risk of identity theft in connection with the opening of covered accounts and with respect to existing covered accounts; significant incidents involving identity theft and the City's response; and recommendations for material changes to the Program. The Program Coordinator shall train staff, as necessary, to effectively implement the Program. The Program Coordinator shall also oversee any service provider arrangements in the event the City engages a service provider to perform an activity in connection with one or more covered accounts to assure that the activity of the service provider is conducted in accordance with this Program and any reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft.