CITY OF EAST LANSING

RED FLAG POLICY AND IDENTITY THEFT PREVENTION PROGRAM
EFFECTIVE: MAY 1, 2009

Purpose

To establish an Identity Theft Prevention 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 the Federal Trade Commission's Red Flags Rule (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.

Under the Red Flag Rules, every financial institution and creditor is required to establish an "Identity Theft Prevention Program" tailored to its size, complexity and the nature of its operation. Each program must contain reasonable policies and procedures to:

1. Identify relevant Red Flags and incorporate them into the Program;
2. Detect Red Flags;
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 or to the safety and soundness of the creditor from Identity Theft.

Definitions

Personal Identification Information means any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including, but not limited to:

- Address and phone number
- Social Security Number (SSN)
- Date of Birth (DOB)
- Government issued Driver’s License, ID or Passport
- Employer or Taxpayer Identification Number
- Internet Protocol address, or routing code
- Credit Card Number
- Bank Account Number
- Student Identification Number
- Alien Registration Number
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, mortgage loans, automobile loans, margin accounts, cell phone accounts, utility 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. (See Appendix A)

Policy

A. PROCEDURES FOR OPENING NEW ACCOUNTS

- In Person:

All new accounts must be set up in person. City personnel will take the following steps to obtain and verify the identity of the person opening the account:

1. Require the customer to present a United States Government or State Government issued photo ID to allow formation of a reasonable belief that the customer is who they claim to be. Photo ID verification is the City’s only acceptable method to confirm a person’s identity. United States Government or State Government issued photo IDs include, but are not limited to:
   - Driver’s License;
   - Military ID; and
   - Passport.

   **NOTE:** Driver’s License or other photo IDs (except passports) issued by a foreign government are not acceptable.

2. Ensure that City personnel’s computer monitors are not visible to others;
3. Ensure that there is no written Personal Identification Information left in view of other customers;
4. Avoid verbal discussion of Personal Identification Information when other customers can overhear the conversation; and
D. RESPONSE TO DETECTING AND IDENTIFYING RED FLAGS

In the event City personnel detect any identified Red Flags, personnel should not confront any individual suspected of committing identity theft. It is only their duty to report any suspected patterns of Identity Theft. Depending on the degree of risk posed by the Red Flag, personnel shall take one or more of the following steps:

1. Continue to monitor an account for evidence of Identity Theft;
2. Contact the customer;
3. Change any passwords or other security devices that permit access to accounts;
4. Not open a new account;
5. Close an existing account;
6. Notify the Privacy Officer for determination of the appropriate step(s) to take;
7. Notify law enforcement if situation warrants; and/or
8. Determine that no response is warranted under the particular circumstances.

F. PROGRAM ADMINISTRATION

The Privacy Officer will appoint a Privacy Committee for the City of East Lansing. The Privacy Officer shall be the Director of Finance. The Committee is headed by the Privacy Officer, with the Assistant Finance Director/Treasurer, Public Works & Environmental Services Director, and Assistant Treasurer comprising the remainder of the committee membership.

The Privacy Officer, with assistance from the Privacy Committee shall:

1. Develop and implement reasonable policies and procedures for an Identity Theft Prevention Program that complies with federal guidelines implementing the FACT Act;
2. Insure all supervisors and employees receive the necessary training to effectively implement the Program;
3. Establish a contact at the East Lansing Police Department to report suspected cases of Identity Theft;
4. Receive reports of Red Flags that require mitigation;
5. Conduct periodic risk assessments of the Program;
6. Periodically review and update the Program procedures and Appendix A – Examples of Red Flags;
7. Ensure continued compliance with the FACT Act;
8. Call meetings of the Privacy Committee as needed or directed by the Privacy Officer to review Policy and Procedures; and
9. Prepare annual reports for the Privacy Officer to present to the City Manager and City Council.

F. PROGRAM UPDATES

This Program will be periodically reviewed and updated to reflect changes in risks to customers and the soundness of the City from Identity Theft. The Privacy Officer will consider the City’s experiences with Identity Theft situations, changes in Identity Theft methods, changes in Identity Theft detection and prevention methods, changes in types of accounts the City maintains and changes in the City’s business arrangements with other entities. After considering these factors,
5. Check for Red Flags. If a Red Flag is detected, follow the prescribed Next Step in the Red Flag check list. If you are unsure of the Next Step, consult with your supervisor before processing the request for the new account. Red Flags must be resolved before a new account can be established.

- **Using Rental Management Company Provided Information:**

Rental management companies or individual landlords requesting service changeovers on behalf of their tenants will be required to submit a form (Attachment 1) which will provide the City with the necessary information for service changeovers, as well as certification from the rental companies that they have verified the identities of the new account holders and the accuracy of the provided data.

**B. PROCEDURES FOR EXISTING ACCOUNTS:**

1. Watch for Red Flags whenever executing transactions on customer accounts;
2. Do not share Personal Identification Information with anyone other than the account holder without the account holder’s permission; and
3. A change of mailing address initiated by the customer must be done in person and requires the same level of authentication as opening a new account.

**C. GENERAL SECURITY GUIDELINES**

In order to further prevent the likelihood of Identity Theft occurring with respect to City accounts, the City will take the following steps with respect to its internal operating procedures to protect customer Personal Identification Information:

1. All employees with access to customer Personal Identification Information are required to complete the Identity Theft Prevention Program training and complete an annual update;
2. Ensure that its website is secure or provide clear notice that the website is not secure;
3. Ensure complete and secure destruction of paper documents and computer files containing customer Personal Identification Information;
4. Ensure that office computers are password protected;
5. Follow proper user ID and password protocol when leaving workstations;
6. Ensure that customer Personal Identification Information is not left on computer screens longer than necessary to execute transactions;
7. Ensure that desks and workstations are clear of papers containing customer Personal Identification Information;
8. Ensure that all computers that have access to customer Personal Identification Information are behind a firewall;
9. Ensure computer virus and spyware protection is up to date; and
10. Require and keep only the kinds of customer Personal Identification Information that are necessary for utility purposes.
the Privacy Officer will determine whether changes to the Program, including the listing of Red Flags, are warranted. If warranted, the Privacy Officer will present to the City Manager and City Council his/her recommended changes and the Council will make determination of whether to accept, modify, or reject those changes to the Program.

G. SPECIFIC PROGRAM ELEMENTS AND CONFIDENTIALITY

For the effectiveness of Identity Theft Prevention Programs, the Red Flag Rule envisions a degree of confidentiality regarding the City’s specific practices relating to Identity Theft detection, prevention, and mitigation. Therefore, under this Program, knowledge of such specific practices shall be limited to the Privacy Committee and those employees who need to know them for purposes of preventing Identity Theft. Because this Program is to be adopted by a public body and thus publicly available, it would be counterproductive to list these specific practices here. Therefore, only the Program’s general Red Flag detection, implementation, and prevention practices are listed in this document.

Authority & Revisions

This policy is enacted immediately upon approval of the City Council, as reflected in the regular meeting minutes dated ____________. Revisions to this policy shall only be enacted when approved by the City Council and reflected in the applicable meeting minutes. This policy shall be reviewed at least biennially by the Privacy Officer and updated as appropriate.

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Revision #</th>
<th>Nature of Revision</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
APPENDIX A – EXAMPLES OF RED FLAGS

I. SUSPICIOUS DOCUMENTS

- Identification document or card that appears to be forged, altered or inauthentic.
- Identification document or card on which a person’s photograph or physical description is not consistent with the person presenting the document.
- Other document with information that is not consistent with existing customer information (example: person’s signature on a check appears forged).
- Application for service that appears to have been altered or forged.

Next Step:
1. In all cases, advise the customer that there appears to be a discrepancy with their documentation and they will need to provide verification of their identity before the transaction can be completed.
2. In some cases, they may need to contact the Secretary of State’s Office to obtain a new document.
3. In some cases, it may be necessary to contact the landlord or property owner to verify who the tenant is.

Mitigation:
1. In all cases, do not open a new account until you are satisfied that the customer is who they claim to be. If necessary, request further documentation (check stub or W-2). Where appropriate attempt to contact the person named on the documents and advise them that they may be the victim of an attempted identity theft. If the matter is not reasonably resolved, advise a supervisor. In some instances, management may need to close an existing account and/or contact the East Lansing Police Department.

II. SUSPICIOUS PERSONAL IDENTIFICATION INFORMATION

- Identifying information presented that is inconsistent with other information the customer provides.
- Identifying information presented that is inconsistent with other sources of information.
- Identifying information presented that is the same as information shown on other applications that were found to be fraudulent.
- Personal ID is inconsistent with utility records.

Next Step:
1. In all cases, advise the customer there appears to be a discrepancy with their documentation and they will have to provide validation of their identity before the transaction can be completed.
2. In some cases, they may need to contact the Secretary of State’s Office to obtain a new document.

Mitigation:
1. Contact the customer, do not open a new account or close an existing account until you have validated the customer’s identity.
III. SUSPICIOUS ACCOUNT ACTIVITY OR UNUSUAL USE OF ACCOUNT

- Change of address for an account followed by a request to change the account holder's name.
- Payments stop on an otherwise consistently up-to-date account.
- Account used in a way that is not consistent with prior use (example: very high activity).
- Mail sent to the account holder is repeatedly returned as undeliverable.
- Notice that a customer is not receiving mail sent by the City.
- Notice that an account has unauthorized activity.

Next Step:
1. Review the account, check for notes and check to see if the customer has been in contact with us.

Mitigation:
1. Contact the customer and advise them of the unusual activity.

IV. NOTICE FROM CUSTOMERS, VICTIMS OF IDENTITY THEFT, LAW ENFORCEMENT AUTHORITIES OR ANY PERSONS REGARDING POSSIBLE IDENTITY THEFT

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

Next Step:
1. Get a copy of the police report and check with the customer to validate their ID and check for accuracy and errors.
2. Review to determine if account should be closed.

Mitigation:
1. Possibly close the account. Contact the customer; change any passwords, security codes or other devices that permit access to the account. Do not attempt to collect on an account until the matter is resolved.
# Table of Red Flags

<table>
<thead>
<tr>
<th>Suspicious Documents</th>
<th>Suspicious Person ID Information</th>
<th>Unusual Use or Suspicious Activity related to the Covered Account</th>
<th>Notice of Theft</th>
</tr>
</thead>
<tbody>
<tr>
<td>Documents provided for ID appeared altered or forged.</td>
<td>Personal ID given by customer is not consistent with other personal ID info.</td>
<td>Change of billing address for an account followed by a request to change the account holder’s name.</td>
<td>Utility is notified by law officials or others, that it has opened a fraudulent account for a person engaged in Identity Theft.</td>
</tr>
<tr>
<td>The photo or physical description is not consistent with the appearance of the applicant.</td>
<td>Personal ID provided is associated with known fraudulent activity. Using same addresses and or phone numbers.</td>
<td>Payments are made in a manner associated with fraud. For example, deposit or initial payment is made and no payments are made thereafter.</td>
<td></td>
</tr>
<tr>
<td>Other information given to open the new account is not consistent with the ID of the applicant.</td>
<td>The customer fails to provide all needed personal ID upon request.</td>
<td>Existing account with a stable history shows irregularities.</td>
<td></td>
</tr>
<tr>
<td>Other information on the ID is not consistent with readily accessible info on file such as signature or recent check.</td>
<td>Personal ID is inconsistent with utility records.</td>
<td>Mail sent to customer is repeatedly returned.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Customer notifies utility that they are not receiving their bill.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>The utility is notified of unauthorized charges or transactions in connection with a customer’s account.</td>
<td></td>
</tr>
</tbody>
</table>
CITY OF EAST LANSING
POLICY RESOLUTION 2009-__

A RESOLUTION ADOPTING A RED FLAG POLICY AND ESTABLISHING AN
IDENTITY THEFT PREVENTION PROGRAM FOR THE CITY OF EAST LANSING

WHEREAS, pursuant to federal law the Federal Trade Commission (the "FTC")
adopted Identity Theft Rules requiring the creation of certain policies relating to the use
of consumer reports, address discrepancy and the detection, prevention and mitigation of
identity theft;

WHEREAS, the FTC regulations, adopted as 16 CFR § 681.2, require creditors,
as defined by 15 U.S.C § 1681a(r)(5), to adopt red flag policies to prevent and mitigate
identity theft with respect to covered accounts;

"creditor" as a person that extends, renews or continues credit, and defines "credit" in
part as the right to purchase property or services and defer payment therefore;

WHEREAS, the FTC regulations include utility companies in the definition of
creditor;

WHEREAS, the City of East Lansing is a creditor with respect to 16 CFR § 681.2
by virtue of providing utility services or by otherwise accepting payment for municipal
services in arrears;

WHEREAS, the FTC regulations define "covered account" in general as an
account that a creditor provides for personal, family or household purposes that is
designed to allow multiple payments or transactions and specifies that a utility account is
a covered account;

WHEREAS, the FTC regulations require each creditor to adopt an Identity Theft
Prevention Program which will use red flags to detect, prevent and mitigate identity theft
related to information used in covered accounts;

WHEREAS, the City of East Lansing provides water, sewer and solid waste
services for which payment is made after the product is consumed or the service has
otherwise been provided which, by virtue of being utility accounts, are covered accounts;

NOW, THEREFORE, BE IT RESOLVED that the City Council of the City of
East Lansing hereby adopts the City of East Lansing Red Flag Policy and Identity Theft
Prevention Program effective May 1, 2009.
Moved by Councilmember:

Supported by Councilmember:

YEAS:
NAYS:

Victor W. Loomis, Jr., Mayor
City of East Lansing

CLERKS CERTIFICATION: I hereby certify that the foregoing is a true and complete copy of a Policy Resolution adopted by the East Lansing City Council at its meeting held on Tuesday, April __, 2009, the original of which is part of the Council's minutes.

Nicole Evans, City Clerk
City of East Lansing