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.

The FTC clarified that a “creditor” includes “lenders such as...utility companies” and indicated that non-profit and governmental entities that defer payments for goods and services should be considered “creditors” for purposes of FACTA.

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:

- Identify relevant Red Flags and incorporate them into the Program;
- Detect Red Flags;
- Respond appropriately to any Red Flags that are detected to prevent and mitigate Identity Theft; and
- 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.

PRIVACY OFFICER / PRIVACY COMMITTEE

The Privacy Officer, with assistance from the Privacy Committee members, is responsible for developing appropriate written procedures and internal controls to assure compliance with the act. The Privacy Officer is responsible for Program Administration.

The Privacy Officer shall be the Administrative Services / Finance Director.

The Privacy Officer will appoint a Privacy Committee for the City of Coldwater and CBPU. The Committee is headed by the Privacy Officer, with the City Accountant / Deputy Clerk, CBPU Director, System Administrator, Public Safety Director and Customer Service Administrator comprising the remainder of the committee membership. The Privacy Officer will be responsible for the Program Administration, for ensuring appropriate training of staff on the Program, for reviewing any staff reports regarding the detection of Red Flags and the steps for preventing and mitigating Identity Theft, determining which steps of prevention and mitigation should be taken in particular circumstances and considering periodic changes to the Program.
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:

- Name
- Address
- Telephone 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
- Personal Identification Number (PIN)
- Bank Account Number
- Utility Account Number

Identify theft is fraud committed using identifying information of another person without authority.

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

POLICY

PROCEDURES FOR OPENING A NEW ACCOUNT

In Person:

1. Obtain sufficient Personal Identification Information to allow you to form a reasonable belief that the customer is who they claim to be, including, but not limited to:
   a. Name
   b. Address
   c. Phone Number
   d. SSN
   e. DOB
   f. Copy of Mortgage, Purchase Agreement or Lease Agreement
   g. United States Government or State Government issued photo ID, driver’s license, military ID or passport (NOTE: Driver’s License or other photo ID’s (except passports) issued by a foreign government are not acceptable.)

2. If a SSN is obtained, then it may be validated with a Credit Agency before it is accepted as proof. SSN’s are a preferred form of identification but are not required. If the
customer prefers not to give their SSN, then they must present acceptable ID in person and may be required to pay a deposit.

3. When obtaining Personal Identification Information in writing from a customer, input the information, immediately shred it or return it to the customer.

4. Avoid taking Personal Identification Information verbally when other customers can overhear the conversation.

5. Ensure that the Customer Service Representatives monitors are not visible to others.

6. 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.

By Telephone:

1. Obtain sufficient Personal Identification Information to allow you to form a reasonable belief that the customer is who they claim to be, including, but not limited to:
   a. SSN
   b. United States Government or State Government used photo ID, driver’s license, military ID or passport. The information on photo ID should be matched against the CRA data when the SSN is validated.
   c. Previous address that matches the CRA data.

2. New Service requests not made in person must include a SSN. Before you accept the SSN as proof of identity you must validate that information by contacting a CRA.

3. Check for Red Flags (See Appendix A: Examples of 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 a new account. Red Flags must be resolved before a new account can be established. If necessary, you should contact the CRA to verify the customer’s identity.

PROCEDURES FOR EXISTING ACCOUNTS

1. Watch for Red Flags whenever executing transactions on customer accounts.

2. Verify the identification of customers if they request information. Do not share account information with anyone other than the account holder without the account holder’s permission and never provide a caller with any personal identification information.

3. A change of mailing address initiated by the customer requires the same level of authentication as opening a new account. Customers must provide personal identification to establish a billing address different than the customer account address.

4. Safeguard all credit card information, checks, ACH information, bankruptcy statements or other personal financial information at all times. These documents should be stored in a secure location until they can be properly destroyed consistent with the Records Retention and Disposal Schedule.
GENERAL SECURITY GUIDELINES

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 information.
4. Avoid including SSN’s in e-mails or written communications. If a SSN is included in an electronic or paper document, that document becomes confidential and must be handled accordingly.
5. Ensure that office computers are password protected and that computer screens lock after a set period of time.
6. Follow proper user ID and password protocol when leaving workstations.
7. Ensure that customers Personal Identification Information is not left on computer screens longer than necessary to execute transactions.
8. Ensure that desks and workstations are clear of papers containing customers Personal Identification Information.
9. Request only the last 4 digits of social security numbers.
10. Ensure that all computers that have access to customer account information are behind a firewall.
11. Ensure computer virus and spyware protection is up to date.
12. Require and keep only the kinds of customer information that are necessary for utility purposes.
13. City of Coldwater and CBPU employee’s personal identification information shall be held to the same security standards as our customer’s information.

RESPONSE TO DETECTING AND IDENTIFYING RED FLAGS

In the event 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 or close an existing account.
5. Notify the Customer Service Administrator for determination of the appropriate step(s) to take.
6. Customer Service Administrator may notify law enforcement if situation warrants.
ADMINISTRATIVE PROCEDURES

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 Coldwater 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. Insure 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.
9. Prepare annual reports for the Privacy Officer to present to the CBPU Director and Board of Directors.

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 of Coldwater and CBPU’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 Identity Theft 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.

Approved by ___________________________________________  ___________
Jeffrey Budd, Finance Director / Privacy Officer  Dated
APPENDIX A – EXAMPLES OF RED FLAGS

I. CRA ALERTS, NOTIFICATIONS & WARNINGS FROM A CONSUMER REPORTING AGENCY (CRA)

• CRA notice of a fraud or active duty alert, credit freeze or address discrepancy.

Next Step:
1. For a fraud or active duty alert request, the customer must come in with photo ID. Review the circumstances with the customer to determine the cause of the alert, notification or warning and verify the customer’s identity.
2. If the CRA reports a credit freeze, review the circumstances with the customer and request that they bring in photo ID. A credit freeze should not affect our ability to verify their identity.
3. For an address discrepancy, notify the customer we need to verify proof of residency with a lease or mortgage. This will be a common occurrence since many customers requesting new service will be in the process of changing addresses.

Mitigation:
1. If a Red Flag is detected while opening a new account, contact the customer and do not open a new account until the customer’s identity and address have been validated.
2. If the Red Flag is detected on an existing account, contact the customer and consider closing the account if the customer’s identity and address cannot be validated.

II. 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 Social Security Administration or 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 Coldwater Police Department.

III. SUSPICIOUS PERSONAL IDENTIFICATION INFORMATION

- Identifying information presented that is inconsistent with other information the customer provides (example: inconsistent birth dates).
- Identifying information presented that is inconsistent with other sources of information (example: an address not matching an address on a credit report).
- Identifying information presented that is the same as information shown on other applications that were found to be fraudulent.
- Identifying information presented that is consistent with fraudulent activity (example: invalid phone number or fictitious billing address).

Next Step:
   1. 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 be completed. In some cases they may need to contact the Social Security Administration or the Secretary of State’s Office to obtain a new document.
   2. In the case of an address discrepancy compared with information from a CRA, require the customer to bring in proper documentation such as a picture ID, pay stub or W2. You must be satisfied the address is correct before proceeding with the transaction.

Mitigation:
   1. Contact the customer, do not open a new account or close an existing account until you have validated the customer’s identity.

- Social security number presented that is the same as one given by another customer

Next Step:
   1. Review the CRA report and compare it to the customer’s description/information. If there is not a good match, then advise the CRA and the customer that there is a discrepancy with their SSN and try to determine the cause of the discrepancy. The customer may need to bring in a photo ID to validate their identity or contact the Social Security Administration if the matter cannot be resolved.
Mitigation:
1. Advise the customer and the CRA of the discrepancy and attempt to contact the person the CRA indicates is the holder of that SSN.
2. Do not proceed with the transaction until you can validate the customer’s identity. Do not open a new account or possibly close an existing account if the customer’s identity cannot be validated.

- An address or phone number presented that is the same as that of another person.

Next Step:
1. Ask customer to verify address / phone number and / or bring in Photo ID.

Mitigation:
1. Do not proceed with any transaction if there is doubt about a customer’s identity.

- A person fails to provide complete personal identifying information on an application or in response to notification that an application is incomplete.

Next Step:
1. Check the billing system for any other customers that may have made a similar attempt to obtain service at that address and ask customer to bring in photo ID.

Mitigation:
1. Do not proceed with any transaction if there is doubt about a customer’s identity.

- A person’s identifying information is not consistent with the information that is on file for the customer or on file with the CRA.

Next Step:
1. Verify all documents to see if the information we have on file is inaccurate. Ask the customer to bring in photo ID and SSN to correct our records.

Mitigation:
1. Do not proceed with any transaction if there is doubt about a customer’s identity.

- In cases where the City of Coldwater and CBPU uses challenge questions and the person cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.

Next Step:
1. Advise the customer that they have failed to provide authenticating information and they must bring in photo ID and SSN to proceed with the transaction.

Mitigation:
1. Do not proceed with any transaction if there is doubt about a customer’s identity.
IV. 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 of Coldwater and CBPU.
- 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.

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

- The City of Coldwater and CBPU is notified by a customer, victim of identity theft, law enforcement authority or any other person that the City of Coldwater and CBPU 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 determinate 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 or sell it to a debt collector until the matter is resolved.

AUTHORITY AND REVISIONS

This policy is enacted immediately upon approval of the Board, as reflected in the regular meeting minutes dated October 21, 2008. Revisions to this policy shall only be enacted when approved by the Board 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>10/16/08</td>
<td>00</td>
<td>Original document</td>
</tr>
<tr>
<td>4/21/09</td>
<td>01</td>
<td>Revised document</td>
</tr>
</tbody>
</table>
# Table of Red Flags per FTC

<table>
<thead>
<tr>
<th>Alerts, Notifications or Warnings from Consumer Reporting Agency</th>
<th>Suspicious Documents</th>
<th>Suspicious Personal ID Information</th>
<th>Unusual Use orSuspicious Activity related to the Covered Account</th>
<th>Notice of Theft</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. A fraud or active duty alert is included with a consumer report.</td>
<td>5. Documents provided for ID appeared altered or forged.</td>
<td>10. Personal ID is inconsistent with external information sources: addresses do not match consumer report; or Social Security Number has not been issued or is listed on the SS Administration Death Master File.</td>
<td>19. Change of billing address is followed by request for adding additional properties to the account (or shortly following the notification of a change in address, the utility receives a request for the addition of authorized users on the account.)</td>
<td>26. 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>2. Consumer reporting agency provides a credit freeze on the customer report.</td>
<td>6. The photo or physical description is not consistent with the appearance of the applicant.</td>
<td>11. Personal ID given by customer is not consistent with other personal ID info. Ex: there is a lack of correlation between the SS# range and DOB.</td>
<td>20. 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>3. Consumer reporting agency provides a notice of address discrepancy.</td>
<td>7. Other information given to open the new account is not consistent with the ID of the applicant.</td>
<td>12. Personal ID provided is associated with known fraudulent activity. Using same addresses and or phone numbers.</td>
<td>21. Existing account with a stable history shows irregularities.</td>
<td></td>
</tr>
<tr>
<td>4. A consumer report indicates a pattern of activity that is inconsistent with the history and usual pattern of activity of an applicant or customer such as:</td>
<td>8. Other information on the identification is not consistent with readily accessible info on file such as signature or recent check.</td>
<td>13. Personal ID is of the same type associated with fraudulent activity: fictitious address, mail box drop or prison or phone number is invalid; it is associated with a pager or answering service.</td>
<td>22. An account with low activity unexpectedly jumps to high consumption. Ex: 1000 kWh to 2801 kWh.</td>
<td></td>
</tr>
<tr>
<td>a) Recent or significant increase in the number of inquiries</td>
<td>9. An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.</td>
<td>14. The SS# is the same as customers opening other accounts.</td>
<td>23. Mail sent to customer is repeatedly returned.</td>
<td></td>
</tr>
<tr>
<td>b) An unusual number of recently established credit relationships</td>
<td></td>
<td>15. The address or phone number is the same as a large number of other applicants.</td>
<td>24. Customer notifies utility that they are not receiving their bill.</td>
<td></td>
</tr>
<tr>
<td>c) Material change in the use of credit especially with respect to new established credit relationships</td>
<td></td>
<td>16. The customer fails to provide all needed personal ID upon request.</td>
<td>25. The utility is notified of unauthorized charges or transactions in connection with a customer’s account.</td>
<td></td>
</tr>
<tr>
<td>d) An account that was closed for cause or identified for abuse of account privileges</td>
<td></td>
<td>17. Personal ID is inconsistent with utility records.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>18. For institutions using challenge questions, the person attempting to access or open account cannot provide any information beyond what would typically be found in a wallet or consumer report.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>