Flathead County
Identity Theft Prevention Program

Program Purpose and Definitions:

The purpose of the Identity Theft Prevention Program ("Program") is to detect, prevent, and mitigate identity theft in connection with billing when Flathead County is considered a creditor. After consideration of the size and complexity of Flathead County's operations, account systems, and the nature and scope of activities, it has been determined this Program is appropriate.

Adopted by Flathead County Board of Commissioners on 6/27/11

This Program contains reasonable policies and procedures to:

1. Identify relevant identity theft triggers for new and existing relevant accounts and incorporate these triggers into the Program;
2. Detect identity theft triggers that have been incorporated into the Program;
3. Respond appropriately to any identity theft triggers 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 Flathead County from identity theft.

The following terms are defined as:

creditor – an entity that allows deferment of payment for goods or services;

identifying information – any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including name, address, telephone number, social security number, date of birth, government issued driver's license or 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.

identity theft – fraud committed using the identifying information of another person;

identity theft trigger – a pattern, practice, or specific activity that indicates the possible existence of identity theft; and

relevant account – an account primarily for personal, family or household purposes, that involves or is designed to permit multiple payments or transactions or any other account for which there is a reasonably foreseeable risk to customers or to the safety and soundness of Flathead County from identity theft;

Identification of Potential Identity Theft Triggers:

In order to identify relevant identity theft triggers, Flathead County considers the types of accounts that it offers and maintains, the methods it provides to open its accounts, the methods it provides to access its accounts, and its previous experiences with identity theft. Flathead County identifies the following identity theft triggers, in each of the listed categories:

Suspicious Documents/Personal Identifying Information – Identity Theft Triggers:

1. Identifying information presented that is inconsistent with other information the customer provides;
2. Identifying information presented that is inconsistent with other sources of information (for instance, an address not matching);
3. Identifying information presented that is consistent with fraudulent activity (such as an invalid phone number or fictitious billing address);
4. An address or phone number presented that is the same as that of another person;

5. A person's identifying information is not consistent with the information that is on file for the customer;
6. Trade/banking reference that is not substantiated.

Suspicious Account Activity or Unusual Use of Account – Identity Theft Triggers:

1. Change of address for an account followed by a request to change the account holder's name;
2. Payments stop on an otherwise consistently up-to-date account;
3. Mail sent to the account holder is repeatedly returned as undeliverable;
4. Notice that a customer is not receiving mail sent by Flathead County;
5. Notice that an account has unauthorized activity;
6. Identified breach in computer system security.

Alerts from Others – Identity Theft Triggers:

Notice to Flathead County from a customer, identity theft victim, law enforcement or other person that it has opened or is maintaining a fraudulent account for a person engaged in identity theft.

Detecting Identity Theft Triggers:

New Accounts:

In order to detect any of the identity theft triggers identified above associated with the opening of a new account, Flathead County personnel will take the following steps to obtain and verify the identity of the person opening the account:

1. Require certain identifying information such as name, date of birth, residential or business address, principal place of business for an entity, driver's license or other identification.
2. Confirming the identification of customer.
3. Independently contact the customer.
4. Review documentation showing the existence of a business entity.
5. Follow up on trade and banking references.

Existing Accounts:

In order to detect any of the identity theft triggers identified above associated with an existing account; Flathead County personnel will take the following steps to monitor transactions with an account:

1. Confirming the identification of customers requesting information by name/account number prior to discussing account information (in person, via telephone, via facsimile, via email).

2. Verifying the validity of requests to change billing addresses by reporting to program administrator an unusually high number of address changes.

3. Verify changes in banking information given for billing and payment purposes.

Preventing and Mitigating Identity Theft:

In the event Flathead County personnel detect any identity theft triggers, such personnel shall take one or more of the following steps, depending on the degree of risk posed by the trigger;

Prevent and Mitigate:

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. Reopen an account with a new number;
7. Notify the Program Administrator for determination of the appropriate step(s) to take;
8. Notify law enforcement; or
9. Determine that no response is warranted under the particular circumstances.

Protect customer identifying information:

In order to further prevent the likelihood of identity theft occurring with respect to County accounts, the County will take the following steps with respect to its internal operating procedures to protect customer identifying information:

1. Ensure that its website is secure or provide clear notice that the website is not secure;
2. Ensure complete and secure destruction of paper documents and computer files containing customer information;
3. Ensure that office computers are password protected and that computer screens lock after a set period of time;
4. Keep offices clear of papers containing customer information;
5. Request only the last 4 digits of social security numbers (if any)
6. Ensure computer virus protection is up to date; and
7. Require and keep only the kinds of customer information that are necessary.

Program Updates:

This Program will be periodically reviewed and updated to reflect changes in risks to customers and the soundness of Flathead County's protection of its customers from identity theft. Periodically, the Program Administrator will review experiences with identity theft situations, changes in identity theft methods, changes in identity theft detection and prevention methods, changes in types of accounts maintained and changes in business arrangements with other entities. After considering these factors, the Program Administrator will determine whether changes to the Program, including the listing of identity theft triggers, are warranted. If warranted, the Program Administrator will recommend modification of the Program to the Flathead County Board of Commissioners.

Program Administration:

Oversight of Program:

The Flathead County Finance Director is the Program Administrator. The Program Administrator will be responsible for the Program development, implementation and administration. This includes ensuring appropriate training of staff, maintaining confidentiality agreements, exercising appropriate and effective oversight of service provider arrangements, reviewing any staff/service provider reports regarding the detection of identity theft triggers and the steps for preventing and mitigating identify theft, determining which steps of prevention and mitigation should be taken in particular circumstances and considering periodic changes in risk or safety to the Program. The Program Administrator will consider other applicable legal requirements as they become applicable.

Staff Training and Reports:

Staff responsible for implementing the Program shall be trained in the detection of identity theft triggers, and responsive steps to be taken when a trigger is detected.

Staff will report to the Program Administrator annually on compliance with the Identity Theft Prevention Program. The report will address material matters related to the Program and evaluate issues such as the effectiveness of the policies and procedures in addressing the risk of identity theft, service provider arrangements, significant incidents involving identity theft and management's response, and recommendations for material changes to the Program.

Oversight of Service Provider Arrangements:

In the event Flathead County engages a service provider to perform an activity in connection with one or more accounts, steps will be taken to ensure the service provider performs its activity in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of Identity theft. Service providers will be required to have such policies and procedures in place to detect relevant identity theft triggers that may arise in the performance of the service provider's activities, and either report the triggers to the Program Administrator, or take appropriate steps to prevent or mitigate identity theft.

Specific Program Elements and Confidentiality:

For the effectiveness of Identity Theft Prevention Programs, there is a degree of confidentiality regarding specific practices relating to identity theft detection, prevention, and mitigation. Therefore, under this Program, knowledge of such specific practices is to be limited to those employees who need to know them for purposes of preventing identity theft.