EXHIBIT A
Identity Theft Protection Program

Definitions. For purposes of the Policy, the following definitions apply (1);

A. 'City' means: the City of Troy, Montana
B. 'Covered Account' means: 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, such as a utility account; and (ii) Any other account that the financial institution or creditor offers or maintains for which there is a reasonably foreseeable risk to customers, of to the safety and soundness of the financial institution or creditor, from identity theft including financial, operational, compliance, reputation or litigation risks.
C. 'Credit' means the right granted by a creditor to a debtor to defer payment of debt or to incur debts and defer its payment or to purchase property or services and defer payment therefore.
D. 'Creditor' means any person who regularly extends, renews or continues credit; any person who regularly arranges for the extension, renewal or continuation of credit, or any assignee of an original creditor who participates in the decision to extend, renew or continue credit and includes utility companies.
E. 'Customer' means a person that has a covered account with a creditor.
F. 'Identity Theft' means a fraud committed or attempted using identifying information of another person without authority.
G. 'Person' means a natural person, a corporation, government or governmental subdivision or agency, trust estate, partnership, cooperative or association.
H. 'Personal Identifying Information' means a person's credit card account information, debit card information, bank account information and driver's license information. For a natural person, it also includes their social security number, mother's birth name and date of birth.
I. 'Red flag' means a pattern, practice or specific activity that indicates the possible existence of identity theft.
J. 'Service provider' means a person that provides a service directly to the City.

Findings

K. The City is a creditor pursuant to 16 CRF 681.2, due to its provision or maintenance of covered accounts for which payment is made in arrears.
L. The processes of opening a new covered account, restoring an existing covered account, making payments on such accounts have been identified as potential processes in which identity theft could occur.
M. The City limits access to personal identifying information to those employees responsible for or otherwise involved in opening or restoring covered accounts or accepting payment for use of covered accounts. Information provided to such employees is entered into the City's Utility Billing system and the contract is filed in a secure area.
N. The City determines that there is a *low risk* of identity theft occurring in the following ways:
    1. Use by an applicant of another person's personal identifying information to establish a new covered account;
    2. Use of a previous customer's personal identifying information by another person, in an effort to have service restored in the previous customer's name;
    3. Use of another person's credit card bank account or other method of payment, by a customer to pay such customer's covered account or accounts;
    4. Use by a customer desiring to restore such customer's covered account, of another person's credit card bank account or other method of payment.

Process of Establishing a Covered Account.

A. As a precondition to opening a covered account in the City, each applicant shall provide the City with any personal identifying information necessary, as may be reasonably requested by

the employee opening said account, to help authenticate customers and monitor account transactions, including address changes. Such information shall be entered into the City's Utility Billing system and the contract then filed in a secure area.

B. Each account shall be assigned an individualized account number based on customer name, billing address and location address.

Access to Covered Account Information.

A. Access to customer accounts shall be limited to authorized City personnel.
B. Any unauthorized access to, or other breach of customer accounts is to be reported immediately to the Operations Supervisor and appropriate actions taken depending on the extent of the breach.
C. Personal identifying information included in customer accounts is considered confidential and any request or demand for such information shall be immediately forwarded to Operations Supervisor and the City Attorney.
D. For any account holder of a covered account, for which the above information is not already on file at city of Troy Utilities, the customer will be contacted within a reasonable period of time, after discovering the missing information, to obtain the necessary information.

Sources and Types of Red Flags

A. All employees responsible for or involved in the process of opening a covered account, restoring a covered account or accepting payment for a covered account, shall check for red flags as indicators of possible identity theft and such red flags may include:

1. Alerts from consumer reporting agencies fraud detection agencies or service providers. Examples of alerts include but are not limited to:

a. A fraud or active duty alert that is included with a consumer report;
b. A notice of credit freeze in response to a request for a consumer report;
c. A notice of address discrepancy provided by consumer reporting agency;
d. Indications of a pattern of activity in a consumer report that is inconsistent with the history and usual pattern of activity of an applicant or customer such as:

i A recent and significant increase in the volume of inquiries;
ii. An unusual number of recently established credit relationships;
iii. A material change in the use of credit, especially with respect to recently established credit relationships; or
iv. An account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor

B. Suspicious documents. Examples of suspicious documents include:

1. Documents provided for identification that appears to be altered or forged:
2. Identification on which the photograph or physical description is inconsistent with the appearance of the applicant or customer;
3. Identification on which the information is inconsistent with information provided by the applicant or customer;
4. Identification on which the information is inconsistent with readily accessible information that is on file with the financial institution or creditor such as a signature card or a recent check; or;
5. An application that appears to have been altered or forged or appears to have been destroyed and reassembled.

C. Suspicious personal identification, such as suspicious address change. Examples of suspicious identifying information include:

1. Personal identifying information that is inconsistent with external information sources used by the financial institution or creditor. For example:
    a. The address does not match any address in the consumer report or
    b. The Social Security Number (SSN) has not been issued or is listed on the Social Security Administration's Death Master File.
2. Personal identifying information provided by the customer is not consistent with other personal identifying information provided by the customer such as a lack of correlation between the SSN range and date of birth.
3. Personal identifying information or a phone number or address is associated with known fraudulent applications or activities as indicated by internal or third party sources used by the financial institution or creditor.
4. Other information provided such as fictitious mailing address, mail drop addresses, jail addresses, invalid phone numbers, pager numbers or answering service is associated with fraudulent activity.
5. The SSN provided is the same as that submitted by other applicants or customers.
6. The address or telephone number provided is the same as or similar to the account number or telephone number submitted by an unusually large number of applicants or customers.
7. The applicant or customer fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete.
8. Personal identifying information is not consistent with personal identifying information that is on file with the financial institution or creditor.
9. The applicant or customer cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.

D. Unusual use of or suspicious activity relating to a covered account. Examples of suspicious activities include:

1. Shortly following the notice of a change of address for an account, City receives a request for the addition of authorized users on the account.
2. A new revolving credit account is used in a manner commonly associated with known patterns or fraud patterns. For example: The customer fails to make the first payment or makes an initial payment, but no subsequent payments.
3. An 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; or, a material change in purchasing or spending patterns.
4. An account that has been inactive for a long period of time is used, taking into consideration the type of account, the expected pattern of usage and other relevant factors.
5. Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's account.
6. The City is notified that the customer is not receiving paper account statements.
7. The City is notified of unauthorized charges or transactions in connection with a customer's account.
8. The City is notified by a customer, law enforcement or another person that it has opened a fraudulent account for a person engaged in identity theft.

E. Notice from customers, law enforcement, victims or other reliable sources regarding possible identity theft or phishing relating to covered accounts.

Prevention and Mitigation of Identity Theft

A. In the event that any City employee responsible for, or involved in an application for a new account becomes aware of red flags indicating possible identity theft with respect to, restoring and existing covered account, or accepting payment for a covered account, such employee shall use their discretion to determine whether such red flag or combination of red

flags suggests a threat of identity theft. If, in their discretion, such employee determines that identity theft or attempted identity theft is likely or probable such employee shall immediately report such red flags to the City Clerk. If, in their discretion, such employee deems that identity theft is unlikely or that reliable information is available to reconcile red flags, the employee shall convey this information to the City Clerk, who may, in their discretion, determine that no further action is necessary. If the City Clerk, in their discretion, determines that further action is necessary, a City employee shall perform one or more of the following responses as determined to be appropriate by the City Clerk:

Application for a new account:

1. Request additional identifying information from the applicant
2. Deny the application for the new account
3. Notify law enforcement of possible identity theft or
4. Take other appropriate action to prevent or mitigate identity theft

Restoring an existing account, or accepting payment for a covered account:

1. Contact the customer.
2. Make the following changes to the account if, after contacting the customer, it is apparent that someone other than the customer has accessed the customer's covered account:
   a. Change any account numbers, passwords, security codes or other security devices that permit access to an account; or
   b. Close the account.
3. Cease attempts to collect additional charges from the customer and decline to sell the customer's account to a debt collector or collections agency in the event that the customer's account has been accessed without authorization and such access has caused additional charges to accrue;
4. Notify a debt collector or collections agency within 72 hours of the discovery of likely or probable identity theft relating to a customer account that has been sold to such debt collector or collections agency in the event that a customer's account has been sold to a debt collector or collections agency prior to the discovery of the likelihood or probability of identity theft relating to such account;
5. Notify law enforcement in the event that someone other than the customer has accessed the customer's account causing additional charges to accrue or accessing personal identifying information; or
6. Take other appropriate action to prevent or mitigate identity theft.

Program Administration

A. The City Clerk/Treasurer is responsible for oversight of the program, and for providing training to all employees responsible for, or involved in, opening a new covered account, restoring an existing covered account, or accepting payment for a covered account with respect to the implementation and requirements of the Identity Theft Prevention Program.
B. The City Clerk/Treasurer will report to the City Attorney at least annually on compliance with the red flag requirements. The report will address material matters related to the program and evaluate issues such as:
   1. The effectiveness of the policies and procedures of the City in addressing the risk of identity theft in connection with the opening of covered accounts and with respect to existing covered accounts
   2. Service provider arrangements
   3. Significant incidents involving identity theft and management response; and
   4. Recommendations for material changes to the Program.
C. The City Attorney is responsible for reviewing reports prepared by the City Clerk regarding compliance with red flag requirements and with recommending material changes to the program as necessary, in their discretion, to address changing identity theft risks and to identify new or discontinued types of covered accounts.

Updating the Program

A. The determination to make changes and update the Administrative Rules for the Identity Theft Prevention Program, along with any relevant red flags in order to reflect changes in risks to customers, or to the safety and soundness of the City and its covered accounts from identity theft will be brought before the City Council for final approval. In doing so, the City Council shall consider the following factors and exercise its discretion in amending the program:
   1. The City's experiences with identity theft;
   2. Updates in methods of identity theft;
   3. updates in customary methods used to detect, prevent and mitigate identity theft;
   4. Updates in the types of accounts that the City offers or maintains; and
   5. Updates in service provider arrangements.

Outside Service Providers

A. In the event that the City engages a service provider to perform an activity in connection with one or more covered accounts, the City Clerk shall exercise their discretion in reviewing such arrangements in order to ensure, to the best of their ability, that the service provider's activities are conducted in accordance with policies and procedures agreed upon by contract that are designed to detect any red flags that may arise in the performance of the service provider's activities and take appropriate steps to prevent or mitigate identity theft.
B. Any contracts entered into with outside service providers will be approved in accordance with City policies regarding contract execution.

Treatment of Address Discrepancies

A. Pursuant to 16 CFR 681.1, the purpose of this section is to establish a process by which the City will be able to form a reasonable belief that a consumer report relates to the consumer about whom it has requested a consumer credit report, when the City has received a notice of address discrepancy.
B. In the event that the City receives a notice of address discrepancy, the City employee responsible for verifying consumer addresses for the purpose of providing the municipal service or account sought by the consumer shall perform one or more of the following activities as determined to be appropriate by such employee:
   1. Compare the information in the consumer report with:
      a. Information the City obtains and uses to verify a consumer's identity in accordance with the requirements of the Customer Information Program rules implementing 31 U.S.C. 5318(1):
      b. Information the Town maintains in its own records such as applications for service change of address notices, other customer account records or tax records; or
      c. Information the City obtains from third party sources that are deemed reliable by the relevant City employee; or
   2. Verify the information in the consumer report with the consumer.

Furnishing Consumers Address to Consumer Reporting Agency

A. In the event that the City reasonably confirms that an address provided by a consumer to the City is accurate, the City is required to provide such address to the consumer-reporting agency from which the City received a notice of address discrepancy with respect to such consumer. Their information is required to be provided to the consumer-reporting agency when:
   1. The City is able to form a reasonable belief that the consumer report relates to the consumer about whom the City requested the report.
   2. The City establishes a continuing relation with the consumer; and

3. The City regularly and in the ordinary course of business provides information to the consumer-reporting agency from which it received the notice of address discrepancy.

B. Such information shall be provided to the consumer-reporting agency as part of the information regularly provided by the City to such agency for the reporting period in which the City establishes a relationship with the customer.

Methods of Confirming Consumer Addresses

A. The City employee charged with confirming consumer addresses may, in their discretion, confirm the accuracy of an address through one or more of the following methods:
   1. Verifying the address with the consumer
   2. Reviewing the City's records to verify the consumers address
   3. Verifying the address through third party sources or
   4. Using other reasonable processes.