CITY OF GOLD BAR, WASHINGTON
RESOLUTION NO. 10-02

A RESOLUTION OF THE CITY COUNCIL OF GOLD BAR, WASHINGTON, ADOPTING AN IDENTITY THEFT PROTECTION PROGRAM.

WHEREAS, the Federal Trade Commission (FTC) has issued regulations defined at "Red Flag" rules requiring financial institutions and creditors to develop and implement written identity theft prevention programs as part of the Fair and Accurate Credit Transactions Act (FACTA) of 2003; and

WHEREAS, the City of Gold Bar maintains certain continuing accounts with water service customers and for other purposes which involve multiple payments or transactions payment deferred until a future date, and which such accounts are defined as "covered accounts" under the Red Flag rules; and

WHEREAS, to comply with the Red Flag rules, the City of Gold Bar has developed an identity theft prevention program to aid in the detection, prevention and mitigation of identity theft in connection with the opening of a "covered account" or an existing "covered account".

NOW THEREFORE, BE IT RESOLVED by the City Council of the City of Gold Bar, Washington as follows:

1. The Identity Theft Prevention Program for the City of Gold Bar, a copy of which is attached hereto as "Exhibit A" and incorporated herein by this reference as if fully set forth, is hereby adopted and approved.

2. The Program Administrator will periodically review and update the Program to reflect changes in risks to customers from identity theft and may amend the policy as required to mitigate identity theft risks to the customers.

RESOLVED this 15th day of June, 2010.

ATTEST/AUTHENTICATED:

Laura Kelly, City Clerk-Treasurer

APPROVED:

Joe Beavers, Mayor

EXHIBIT A

Identity Theft Prevention Program

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 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.

Definitions
Identity theft is fraud committed or attempted using the identifying information of another person without authority.

A **covered account** is defined as:

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** is a pattern, practice or specific activity that indicates the possible existence of identity theft.

Identifying information is defined as any name or number that may be used alone or 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.

The Program
The City of Gold Bar establishes an Identity Theft Prevention Program to detect, prevent and mitigate identity theft. The Program shall include reasonable policies and procedures to:

- Indentify relevant Red Flags for covered accounts that it offers or maintains and incorporate those Red Flags into the Program.
- Detect Red Flags that have been incorporated into the Program.
- Respond appropriately to any Red Flags that are detected to prevent and mitigate identity theft.
- Ensure that the Program is updated periodically to reflect any changes in risk to the customers and to the safety and soundness of the creditor from identity theft.

The Program shall, as appropriate, incorporate existing policies and procedures that control reasonably foreseeable risks.

Identification of Red Flags
The Program shall include relevant Red Flags from the following categories as appropriate:

- Alerts, notifications, or other warnings received from consumer reporting agencies or service providers, such as fraud detection services.
- The presentation of suspicious documents.
- The presentation of suspicious personal identifying information.
- The unusual use of, or other suspicious activity related to, a covered account.
- Notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts.

The Program shall consider the following risk factors in identifying relevant Red Flags for covered accounts as appropriate:

- The types of covered accounts offered or maintained.
- The methods provided to open covered accounts.
- The methods provided to access covered accounts.
- Any previous experience with identity theft.

The Program shall incorporate relevant Red Flags from sources such as:

- Incidents of identity theft previously experienced.
- Methods of identity theft that reflect changes in risk.
- Applicable supervisory guidance.

Detection of Red Flags
The City of Gold Bar identifies the following Red Flags and will train the appropriate staff to recognize these Red Flags as they are encountered in the ordinary course of city business:

Suspicious Documents
- Identification document or card that appears to be forged, altered or unauthentic.
- Identification document or card where a person's photograph or physical description is not consistent with the person presenting the document.
- Other information on the identification document is not consistent with the information provided by the person opening a new covered account, by the customer presenting the identification, or with existing customer information on file with the creditor (such as a signature card or recent check).
- Application for service that appears to have been altered or forged.

Suspicious Personal Identifying Information
- Identifying information presented that is inconsistent with other information that the customer provides, for instance, where there is a lack of correlation between the social security number range and the date of birth.
- Identifying information presented that is inconsistent with external sources of information, for instance, an address does not match a consumer report or a social security number is listed in the Social Security Administration's Death Master File.
- Identifying information presented is associated with common types of fraudulent activity such as use of a fictitious billing address or phone number.
- Identifying information presented is consistent with known fraudulent activity, such as the presentation of an invalid phone number or fictitious billing address used in previous fraudulent activity.
- Social security number presented is the same number that has been given by another customer.
- An address or phone number presented that is the same as that of another person.
- A person fails to provide complete personal identifying information on an application when reminded to do so (however, by law, social security numbers must not be required).
- A person's identifying information is not consistent with the information that is on file for the customer.

Suspicious Account Activity or Unusual Use of An 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 to the City that a customer is not receiving mail sent by the City.
- Notice to the City that an account has had unauthorized activity.

- Breach in the City's computer system security.
- Unauthorized access to or use of customer account information.

Alerts from Others

- Notification to the City from a customer, identity theft victim, law enforcement officer, or another person that it has opened or is maintaining a fraudulent account for a person engaged in identity theft.

Preventing and Mitigating Identity Theft

In the event that City personnel detect any identified Red Flags, such personnel must contact the City Clerk/Treasurer. The City Clerk/Treasurer will then decide which of the following steps should be taken:

1) Monitor the covered account for evidence of identity theft.
2) Contact the customer.
3) Change any passwords, security codes, or other security devices that permit access to a covered account.
4) Reopen a covered account with a new account number.
5) Not open a new covered account.
6) Close an existing covered account.
7) Notify law enforcement.
8) Determine that no response is warranted under the particular circumstances.

Program Updates

The Utility Clerk, or designee, shall serve as the Program Administrator. The Program Administrator will periodically review and update this Program to reflect any changes in risk to the customers or to the safety and soundness of the organization from identity theft based on factors such as:

- The experiences of the organization with identity theft.
- Changes in methods of identity theft.
- Changes in methods to detect, prevent, and mitigate identity theft.
- Changes in the types of accounts that the organization offers or maintains.
- Changes in the business arrangements of the organization, including mergers, acquisitions, alliances, joint ventures, and service provider arrangements.

After considering these factors, the Program Administrator will determine whether changes to the Program, including the listing of Red Flags, are warranted. If warranted, the Program Administrator will update the Program or present the City Council with recommended changes and the City Council will make a determination of whether to accept, modify, or reject those changes to the Program.

Administration of Program

- The Program Administrator shall be responsible for the development, implementation, oversight, and continued administration of the Program.
- The Program shall include staff training, as necessary, to effectively implement the Program.
- The Program shall include appropriate and effective oversight of service provider arrangements.

Oversight of the Program

Oversight of the Program shall include:

- Implementation of the Program.
- Review of reports prepared by staff regarding compliance.
- Approval of material changes to the Program as necessary to address the changing risks of identity theft.

Reports shall be prepared as follows:

- The staff responsible for development, implementation, and administration of the Program shall report to the Program Administrator annually, at least, regarding compliance by the organization to the Program.
- The report shall include matters related to the Program such as:

    1) The effectiveness of the policies and procedures in addressing the risk of identity theft as it relates to the opening of covered accounts and existing covered accounts.
    2) Service provider agreements.
    3) Significant incidents involving identity theft and management's response.
    4) Recommendations for material changes to the Program.

Oversight of Service Provider Arrangements

The City shall take steps to ensure that the activity of a service provider is conducted in accordance with reasonable policies and procedures designed to detect, prevent and mitigate the risk of identity theft whenever the organization engages a service provider to perform an activity in connection with one or more covered accounts.