CITY OF HEALDSBURG ADMINISTRATIVE DIRECTIVE	
SUBJECT: IDENTITY THEFT PREVENTION	**NUMBER: FIN – 105.3**
EFFECTIVE DATE: NOVEMBER 3, 2008	**COUNCIL ADOPTION:**
AMENDS/SUPERSEDES:	**APPROVED:** MARJIE PETTUS, CITY MANAGER

IDENTITY THEFT PREVENTION POLICY

I. PROGRAM INTRODUCTION

This Identity Theft Prevention Program ("Program") is developed and implemented pursuant to the Fair and Accurate Credit Transactions Act of 2003 ("FACTA"), 15 U.S.C. 1681 *et seq.*, and regulations of the Federal Trade Commission ("FTC") known as the "Red Flag Rules" ("Rules"), 16. C.F.R. Part 681 that were designed and adopted in compliance with FACTA. The Rules require the City of Healdsburg ("City") to develop and implement a program to detect, prevent and mitigate identity theft. This Program is intended to memorialize and outline the identity protections and procedures of the City and to formalize their continued use and update, as required by law.

II. PROGRAM PURPOSE

A. The City places the highest priority on protecting any confidential financial and personal information submitted to it in the course of providing City services. This Program applies to the water, sewer and electric utility accounts, first-time homebuyers' loan accounts, recreation program accounts and any other accounts that may be offered and maintained by the City requiring information that may lead to identity theft.

B. This Program has the following purposes:

1. Identity "red flags" applicable to the accounts offered and maintained by the City and incorporate those "red flags" into this Program.
2. Detect those "red flags" that have been incorporated into this Program as they occur.
3. Ensure that staff responds appropriately to detected "red flags" so as to prevent and mitigate identity theft.
4. Ensure that this Program is updated periodically to reflect changes in identity theft risk to City customers or to the City.
5. Ensure that all service providers' activities are conducted in accordance with reasonable policies and procedures to detect, prevent and mitigate the risk of identity theft.

III. DEFINITIONS

For purposes of this Program, the words set forth below shall have the following meanings:

1. "Account" means the water, sewer and electric utility accounts, first-time homebuyers' loan accounts, recreation program accounts and any other accounts that may be offered and maintained by the City requiring information that may lead to identity theft. These accounts qualify as "accounts" and "covered accounts" as defined by the Rules under 16

C.F.R. section 681.2.

2. "Customer" means a person that is applying to open an account or a person that has an existing account with the City.

3. "Identifying information" means any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including any:

   (a) Name, Social Security Number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number; unique electronic identification number, address, or routing code, or as otherwise provided in 16 C.F.R. section 603.2.

4. "Identity theft" means a fraud committed or attempted using the identifying information of another person without authority or as otherwise provided in 16 C.F.R. section 603.2.

5. "Person" means a natural person, a corporation, government or governmental subdivision or agency, trust, estate, partnership, cooperative, or association.

6. "Red flag" means a pattern, practice, or specific activity that indicates the possible existence of identity theft.

7. "Service Provider" means a person that provides a service directly to the City in connection with one or more accounts.

8. "Staff" means the City staff who has access to identifying information of customers during the opening and maintaining of the accounts.

IV. IDENTIFICATION OF RED FLAGS

A. The City has completed an assessment of the accounts it offers and maintains to determine potential red flags that may arise in connection to the accounts. The City has assessed the following: (1) the type(s) of Accounts offered and maintained by the City; (2) the methods the City uses to open accounts; (3) the methods it provides to allow Staff and customers to access accounts; and (4) the City's previous experiences with identity theft.

B. Based on the foregoing assessment, the City has determined that the existence of any of the following red flags in connection with any account indicates the possible existence of identity theft:

1. Suspicious Documents

(a) Documents provided by the customer for identification appear to have been altered or forged.

(b) The photograph or physical description on the identification is not consistent with the appearance of the customer presenting the identification.

(c) Other information on the identification is not consistent with information provided by the customer.

(d) Other information on the identification is not consistent with readily accessible information that is on file with the City, such as a signature card or a recent check.

(e) An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

2. Suspicious Customer Identifying Information

(a) The identifying information provided by the customer is inconsistent when compared against external information sources used by the City. For example:

(i) The Social Security Number has not been issued, or is listed on the Social Security Administration's Death Master File.

(b) The identifying information provided by the customer is inconsistent with other personal identifying information provided by the customer. For example, there is a lack of correlation between the Social Security Number range and date of birth.

(c) The identifying information provided by the customer is associated with known fraudulent activity as indicated by internal or third-party sources used by the City. For example, the address or phone number on an application is the same as the address or phone number provided on a fraudulent application.

(d) The identifying information provided by the customer is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the City. For example:

(i) The address on an application is fictitious, a mail drop, or a prison; or

(ii) The phone number is invalid, or is associated with a pager or answering service.

(e) The Social Security Number provided by the customer is the same as that submitted by other customers opening accounts or having existing accounts with the City.

(f) The address or telephone number provided by the customer is the same as or similar to the address or telephone number submitted by an unusually large number of other customers opening accounts or having existing accounts with the City.

(g) A customer opening an account or having an existing account fails to provide all required identifying information on an application or in response to notification that the application is incomplete.

(h) The customer identifying information is not consistent with identifying information that is on file with the City.

(i) A customer opening an account or having an existing account cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report. For example, the customer cannot answer a challenge question.

3. Suspicious Activity

(a) Shortly following receipt of a notice of a change of address from a customer for their account, the City receives additional requests for changes to the account.

(b) An account is used in a manner that is not consistent with established patterns of activity on the account. For example, the customer misses a payment when there is no history of late or missed payments.

(c) Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's account.

(d) The City is notified that the customer is not receiving paper account statements or billing

statements.

(e) The City is notified of unauthorized transactions in connection with a customer's account.

4. Notices From Customers, Victims of Identity Theft, Law Enforcement Authorities, or Other persons

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

V. DETECTION OF RED FLAGS

A. In connection with the opening and maintaining of any account, staff shall take the steps set forth below to detect red flags.

B. Opening New Accounts:

1. Staff shall verify the identity of each customer to the extent reasonable and practicable.

2. Staff shall obtain the following identifying information to verify the identity of each customer: name of the customer, date of birth for individuals, address, taxpayer identification number, driver's license number or Social Security Number.

3. Staff shall review the obtained identifying information for any red flags identified in Section IV of this Program.

4. Staff shall obtain a copy of any of the following documents verifying the identifying information submitted by each customer: driver's license, passport, government-issued identification card, articles of incorporation, a government-issued business license, a partnership agreement, or trust.

5. Staff shall review the obtained copies of documents verifying the identifying information submitted by each customer for any red flags identified in Section IV of this Program.

6. Staff shall verify the customer's identity through the comparison of the identifying information and any other information provided by the customer with information contained in City files or information obtained from any other source.

7. If the customer is not an individual and staff cannot verify the customer's identity through the steps listed above, staff may, based on a risk assessment, obtain identifying information of and verify the identity of the individuals with authority or control over the account, including signatories, pursuant to the steps listed above.

C. Maintaining Existing Accounts:

1. Staff shall verify the identity of each customer that requests account information, other than a request for the outstanding balance owed, to the extent reasonable and practicable.

2. Staff shall monitor the transactions of the Accounts maintained by the City for any red flags identified in Section IV of this Program.

3. Staff shall verify the validity of any notice of change of address or notice of change of billing information by contacting the customer and/or through the comparison of the identifying information in the notice of change of address or notice of change of billing information and any other information provided by the customer with information

contained in City files, or information obtained from any other source.

VI. PREVENTING AND MITIGATING IDENTITY THEFT

A. In the event that staff detects any red flags related to an account, staff shall respond to the red flag by taking one or more of the responsive actions set forth below. In responding to a red flag, staff shall take into consideration which actions are appropriate for the degree of risk of identity theft posed by the red flag.

B. Responses to Detected Red Flags

1. Mark an account in the billing system and monitor it for evidence of identity theft.
2. Contact the customer.
3. Change any passwords, security codes or other security devices that permit access to an account.
4. Reopen an account with a new account number.
5. Refuse to open a new account.
6. Close an existing account.
7. Not attempt to collect on an account or not sell the account to a debt collector.
8. Notify law enforcement and/or prosecutorial agencies.
9. Determine that no response is warranted under the particular circumstances.
10. Notify the Finance Director for determination of the appropriate step(s) to take.

C. Each situation shall be evaluated on a case-by-case basis. In determining an appropriate response, Staff shall consider any aggravating factors that may heighten the risk of identity theft. For example, a data security incident that results in unauthorized access to a customer's account records held by the City, receipt of notice that a data security incident has occurred that results in unauthorized access to a customer's account records held by a third-party, or receipt of notice that a customer has provided information relating to an account with the City to someone fraudulently claiming to represent the City or to a fraudulent website.

D. Internal Protection of Customer Identifying Information

1. In order to further prevent the likelihood of identity theft occurring with respect to Accounts offered and maintained by the City, Staff shall take the following steps with respect to its internal operation procedures to protect customer identifying information:

(a) Ensure that its website is secure or provide clear notice that the website is not secure.

(b) Ensure that office computers from which customer identifying information may be accessed are password protected.

(c) Keep all desks, workstations, work areas, printers, fax machines and common shared work areas clear of documents containing customer identifying information when not in use.

(d) Ensure computer virus protection is up to date.

(e) Lock all file cabinets, desk drawers, overhead cabinets and any other storage space containing documents with customer identifying information when not in use.

(f) Lock storage rooms containing documents with customer identifying information at the end of each workday or when unsupervised.

VII. ADMINISTRATION AND UPDATING OF THIS PROGRAM

A. This Program shall be administered by the Finance Director.

1. The Finance Director shall be responsible for:

(a) Assigning the specific responsibility for this Program's implementation to the appropriate staff.

(b) Review annual reports prepared by staff regarding compliance by the City with FACTA and the Rules.

(c) Approve material changes to this Program as necessary to address changing identity theft risks.

B. Annual Reports

1. Staff shall provide annual reports to the Finance Director regarding compliance of this Program with the Rules.

2. The annual reports shall address any material matters related to this Program and evaluate any issues related to this Program, including:

(a) The effectiveness of this Program in addressing the risk of identity theft in connection with the opening and maintaining of accounts.

(b) Any arrangements with new service providers or any changes in the arrangements with existing service providers to detect, prevent and mitigate identity theft, if applicable.

(c) Any significant incidents involving identity theft and staff's response to those incidents.

(d) Changes in methods of identity theft.

(e) Changes in methods to detect, prevent and mitigate identity theft.

(f) Changes in the types of accounts the City offers or maintains.

(g) Recommendations for material changes to this Program.

C. Updating this Program

1. Upon review of the annual reports submitted by staff and the recommendations contained therein, the Finance Director shall determine whether material changes to this Program are necessary to update this Program to better detect, prevent and mitigate identity theft related to the accounts offered and maintained by the City.

2. If the Finance Director determines that such an update to this Program is necessary, the Finance Director shall direct staff to draft the recommended material change(s) to this Program, which shall be submitted to the City Council for approval.

D. Staff Training

1. The Finance Director shall ensure that Staff is trained as necessary to effectively

implement this Program, which includes training regarding any approved material changes to this Program.

VIII. OVERSIGHT OF SERVICE PROVIDERS

A. The City shall take steps necessary to ensure that the activity of any service provider is conducted in accordance with reasonable policies and procedures designed to detect, prevent and mitigate the risk of identity theft.

B. The Finance Director shall determine which steps are necessary to ensure the activities of any service providers are conducted in accordance with reasonable policies and procedures designed to detect, prevent and mitigate the risk of identity theft. The Finance Director may, if he or she deems it appropriate, require a service provider by contract to design and implement policies and procedures to detect relevant red flags that may arise in the performance of the Service Provider's activities related to the accounts, and either report the red flags to the Finance Director or to take appropriate steps to prevent or mitigate identity theft.

REVIEW AND REVISION

The City of Healdsburg reserves the right to rescind and/or amend this and all City policies, at any time.