

## 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