SUBJECT: Identity Theft "Red Flag" Program

DATE ISSUED: August 21, 2018

SECTION: I

I. PROGRAM ADOPTION

The City of Tracy ("City") developed this Identity Theft Prevention Program ("Program") in accordance with the Federal Trade Commission's Identity Theft Rules ("Red Flag Rule"), which implements Section 114 of the Fair and Accurate Credit Transactions Act of 2003 ("FACTA"). 16 CFR § 681.1(d). This Program also incorporates the Red Flag Protection Clarification Act of 2010 ("Clarification Act") and 16 CFR 682.3 of FACTA ("Disposal Rules"). This Program was approved by the City Council on August 21, 2018.

II. PURPOSE

Pursuant to federal regulations, the City is a creditor because it provides services to customers prior to receipt of payment through customer accounts, including utility service accounts, which are maintained primarily for personal, family, or household purposes and involve multiple payments or transactions, and for which there is a foreseeable risk of identity theft. As a creditor, the City is required to implement an Identity Theft Protection Program.

III. DEFINITIONS

Red Flags, means and refers to, "a pattern, practice, or specific activity that indicates the possible existence of identity theft," as defined in 16 CFR § 601.1(b)(ii)(9).

Covered Account(s), means and refers to, any account the City offers or maintains that involves or is designated to permit multiple payments or transactions, and any other account the City offers or maintains for which there is a reasonably foreseeable risk to customers, employees, or citizens or to the safety and soundness of the City from Identity Theft. Covered Account(s) is further defined in Section V.C. below.

Customer, means and refers to, a person that has a Covered Account(s) with the City.

Dispose, Disposing, or Disposal, means and refers to, the discarding or abandonment of personal identifying information; or the sale, donation, or transfer of any medium, including computer equipment, upon which personal identifying information is stored.

Identity Theft, means and refers to, "fraud committed using the identifying information of another person," as defined in 16 CFR 603.2(a).

Personal identifying information, means and refers to, information that may be used to identify a specific person, including, but not limited to, a social security number, date of birth, government issued driver's license or identification number, government passport number, any unique electronic identification number, telephone number or address.

IV. DESIGNATION OF AUTHORITY

The City Council designates the authority to develop, oversee, implement, and administer the Program to the Finance Director or designee.

As part of the Finance Director's oversight responsibilities for the Program, the Finance Director or designee is required to review and approve all material changes to the Program as necessary to address changing identity theft risks.

V. REQUIREMENTS OF THE RED FLAG AND DISPOSAL RULES

A. Red Flags Rule

The City's Program should be designed to detect, prevent, and mitigate identity theft in connection with opening of a covered account or any existing covered account. The Program must be appropriate to the size, complexity and the nature of its operation. The Program must include reasonable policies and procedures to:

(1) Identify Red Flags for the covered accounts that the City offers and incorporate those Red Flags into its Program,

(2) Detect Red Flags that have been incorporated into the City's Program,

(3) Respond appropriately to any Red Flags 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 the creditor from Identity Theft

B. Disposal Rule

Any government agency that maintains or otherwise possesses personal identifying information for a business purpose must properly dispose of such information by taking reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal.

C. Covered Account(s)

The City is a creditor for the purposes of FACTA and has determined that it maintains the following Covered Account(s):

1. Utility Accounts
2. Miscellaneous Accounts Receivables
3. Home Loan Receivables

VI. IDENTIFICATION OF RED FLAGS

To identify the Red Flags applicable to the City's Consumer Account(s), the City considers the following Red Flags:

A. Notifications and Warnings from Credit Reporting Agencies

Red Flags

- Alerts, notifications or warnings from a consumer reporting agency;
- A fraud or active duty alert included with a consumer report;
- A notice of credit freeze from a consumer reporting agency in response to a request for a consumer report; or
- A notice of address discrepancy from a consumer reporting agency as defined in § 334.82(b) of the FACTA.

Red flags also include consumer reports that indicate a pattern of activity inconsistent with the history and usual pattern of activity of an applicant or customer, such as:

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

B. Suspicious Documents

Red Flags

- Documents provided for identification that appear to have been altered or forged.
- The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.
- Other information on the identification is not consistent with information provided by the person opening a new account or customer presenting the identification.
- 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.
- An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

C. Suspicious Personal Identifying Information

Red Flags

Personal identifying information provided is inconsistent when compared against external information sources used by the City. For example:

- The address does not match any address in the consumer report; or
- The Social Security number (SSN) has not been issued or is listed on the Social Security Administration's Death Master File; or
- Personal identifying information provided by the customer is not consistent with other personal identifying information provided by the customer. For example, there is a lack of correlation between the SSN range and date of birth.

Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the City. For example:

- The address on an application is the same as the address provided on a fraudulent application; or
- The phone number on an application is the same as the number provided on a fraudulent application.

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

- The address on an application is fictitious, a mail drop, or a prison; or
- The phone number is invalid or is associated with a pager or answering service.
- The SSN provided is the same as that submitted by other persons opening an account or other customers.
- The address or telephone number provided is the same as or similar to the address or telephone number submitted by an unusually large number of other customers or other persons opening accounts.
- The customer or the person opening the account fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete.
- Personal identifying information provided is not consistent with personal identifying information that is on file with the City.
- When using security questions (mother's maiden name, pet's name, etc.), the person opening the Covered Account(s) or the 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 related to, Covered Account(s)

Red Flags

Shortly following the notice of a change of address for an account, the City receives a request for new, additional, or replacement goods or services, or for the addition of authorized users on the account.

A new revolving credit account is used in a manner commonly associated with known patterns of fraud patterns. For example:

- The customer fails to make the first payment or makes an initial payment but no subsequent payments.

A Covered Account(s) 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;
- A material change in purchasing or usage patterns

A Covered Account(s) that has been inactive for a reasonably lengthy period of time is used (taking into consideration the type of account, the expected pattern of usage and other relevant factors).

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

The City is notified of unauthorized charges or transactions in connection with a customer's Covered Account(s).

E. Alerts from Others

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

VII. DETECTING RED FLAGS

The City uses the following procedures to detect Red Flags identified with opening of accounts and existing accounts.

New Accounts:

- Obtain personal identifying information of an individual to verify his/her identity prior to opening an account.
- Authenticate the identity of customers when they are requesting information about their accounts.
- Review documentation showing the existence of a business entity (example: presentation of a business card, business letterhead, or business license); and
- Independently contact the affected customer if appropriate.

Existing Accounts:

- Verify the identification of customers if they request information (in person, via telephone, via fax, via email).
- Verify the validity of all billing address change requests.
- Verify all requested change to banking information used for payment purposes.

VIII. PREVENTING AND MITIGATING IDENTITY THEFT

If City personnel detect any identified Red Flags, such personnel shall take on or more of the following steps, depending on the degree of risk posed by the Red Flag:

A. Hard Copy Distribution

Each employee and consultant will comply with the following policies:

- File cabinets, desk drawers, overhead cabinets, and any other storage space containing documents with personal identifying information will be locked when not in use.
- Storage rooms containing documents with personal identifying information and record retention areas will be locked at the end of each workday or when unsupervised.
- Desks, workstations, work areas, printers and fax machines, and common shared work areas will be cleared of all documents containing personal identifying information when not in use.
- All computers containing personal identifying information will be locked when not in use.

B. Electronic Distribution

Each employee and consultant performing work for the City of Tracy will comply with the following policy:

- Internally, personal identifying information may be transmitted using approved email.
- Any personal identifying information sent externally must be sent only to approved recipients.
    - Additionally, a statement such as this should be included in all City e-mails: "This email may contain personal identifying information that is subject to protection under state and federal law. This information is intended for the use of the individual named above. If you are not the intended recipient, be aware that any disclosure, copying, distribution or use of the contents of this information is prohibited and may be punishable by law. If you have received this electronic transmission in error, please notify us immediately by electronic mail (reply)."

C. Employee & Consultant Notification

Periodic email notifications of this policy, no less than once per year, will be sent to all City employees and consultants performing work for the City.

D. Responding To Red Flags

Once identified Red Flags are detected, an employee must act quickly as a rapid appropriate response can protect customers and the City from damages and loss. When activity is detected, gather all related documentation and write a description of the situation. Present this information to the Finance Director or designee for determination. The Finance Director or designee will complete additional authentication to determine whether the attempted transaction was fraudulent or authentic. If a transaction is determined to be fraudulent, appropriate actions must be taken immediately. Actions may include:

- Canceling the transaction;
- Notifying and cooperating with appropriate law enforcement;
- Determining the extent of liability of the City; and

- Notifying the actual customer that fraud has been attempted.

E. Proper Disposal of Personal Identifying Information

The City will take reasonable measures to protect against unauthorized access to or use of personal identifying information. The following steps will be taken:

- Require City personnel or reputable destruction service provider to shred papers containing personal identifying information so that the information cannot practicably be read or reconstructed;
- Require City personnel or reputable destruction service provider to destruct or erase electronic media containing personal identifying information so that the information cannot practicably be read or reconstructed;
- Prohibit City personnel or service provider from selling, donating, or transferring any medium, including computer equipment, upon which personal identifying information is stored.

IX. Program Updates

At periodic intervals established in the program, or as required, the program will be re-evaluated to determine whether all aspects of the program are up to date and applicable in the current business environment. Periodic reviews will include an assessment of which accounts are covered by the program. As part of the review, Red Flags may be revised, replaced or eliminated. Defining new Red Flags may also be appropriate. Actions to take in the event that fraudulent activity is discovered may also require revision to reduce damage to the City and its customers.