

City of Fresno
RED FLAG PROGRAM--POLICY AND
PROCEDURES



Effective MAY 1, 2009

Karen M. Bradley, CPA
Interim Controller

PURPOSE

To establish uniform policies and procedures in order to implement an anti-identity theft program, in compliance with the joint rules (the “guidelines”) issued by the U.S. Department of the Treasury, Office of the Comptroller of the Currency and Office of Thrift Supervision, the Federal Reserve System, the Federal Deposit Insurance Corporation, the National Credit Union Administration, and the Federal Trade Commission (the “Agencies”), in accordance with the Fair and Accurate Credit Transactions Act of 2003 (“FACTA”), known as the Identity Theft Red Flags and Address Discrepancies law.

POLICY

It shall be the Policy of the City of Fresno (the “City”) to proactively endeavor to reduce and eliminate, insofar as possible, the crime of identity theft, by adopting and implementing a program designed to detect, prevent, and mitigate identity theft, in connection with the opening of certain accounts or certain existing accounts with the City. This program shall constitute a written Identity Theft Prevention Program (the “Program”) intended to constitute reasonable policies and procedures that will comply with the guidelines issued by the aforementioned Agencies, in connection with the implementation of FACTA. This program shall be known as the City of Fresno Anti-Identity Theft Red Flags Program, (the “Red Flags Program”).

PROCEDURES

Definitions

Account:	a continuing relationship established by a person with the City of Fresno to obtain a product or service for personal, family, household or business purposes. Account includes an extension of credit, such as the purchase of property or services involving a deferred payment and a deposit account.
Board of Directors:	the governing board of a creditor, here the City Council.
Covered Account:	an account that a creditor offers, primarily for personal, family, or household purposes, that is designed to permit multiple payments or transactions, such as a utility account, and any other account that the creditor offers for which there is a reasonably foreseeable risk to customers or to the creditor from identity theft, including financial, operational, compliance, reputation, or litigations risks.
Credit:	the right granted by a creditor to a debtor to defer payment of debt or to incur debts and defer payment or to purchase property or services and defer payment therefore.
Creditor:	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 extending, renewing, or continuing credit.

Customer:	a person that has a covered account with a creditor.
Identity Theft:	the taking of a victim's identity to obtain credit and credit cards from banks and retailers, steal money from a victim's existing accounts, apply for loans, establish accounts with utility companies, rent an apartment, file bankruptcy, or obtain a job using the victim's name.
Identifying Information:	any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including any 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 biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation; unique electronic identification number, address, or routing code; or telecommunication identifying information or access device.
Notice of Address Discrepancy:	a notice sent to a user by a consumer reporting agency that informs the user of a substantial difference between the address for the consumer that the user provided to request the consumer report and the address(es) in the agency's file for the consumer.
Red Flag:	a pattern, practice, or specific activity that indicates the possible existence of identity theft.
Red Flag Administrator:	City Manager/designee(s) thereof .
Red Flag Officer:	Departmental representative responsible for administration and oversight of the City's Red Flag Program within their Department.
Red Flag Task Force:	key City staff responsible for the oversight and administration of the City's Red Flag Program.
Service Provider:	a person that provides a service directly to the creditor.

Key Elements of the Program

The Red Flag Program shall include the following four key elements:

1. Identifying relevant Red Flags for new and existing covered accounts and incorporating those Red Flags into the Program;
2. Detecting Red Flags that have been incorporated into the Program;

3. Responding appropriately to any Red Flags that are detected to prevent and mitigate Identity Theft; and
4. Ensuring the Program is updated periodically, to reflect changes in risks to customers or to the safety and soundness of the City from Identity Theft.

Identification of Red Flags

The key to the Red Flag Program is the identification of Red Flags. These may occur in an obvious and clear manner. On the other hand, Red Flags may be subtle and difficult to identify. It is important for staff to maintain an attitude of professional skepticism with regard to any proof or evidence of identity, regardless of what is presented. The City shall utilize the operating definition of identifying information listed above. In addition to standard identifying information, Departments are encouraged to utilize public and/or proprietary databases to verify the identity of persons wishing to open new accounts with the City. In the case of accounts that already exist, staff must be vigilant with regard to unusual activity that might be indicative of an attempt at identity theft.

The following shall be regarded as Red Flags for staff, indicative of a possible attempt at Identify Theft, whenever a new account is being requested:

- A. Notifications and Warnings From Credit Reporting Agencies
 1. A fraud or active duty alert is included with a consumer report
 2. A consumer reporting agency provides a notice of credit freeze in response to a request for a consumer report
 3. A consumer reporting agency provides a notice of address discrepancy
 4. A consumer report indicates a pattern of activity that is inconsistent with the history and usual pattern of activity of an applicant or customer, such as:
 - a. A recent and significant increase in the volume of inquiries
 - b. An unusual number of recently established credit relationships
 - c. A material change in the use of credit, especially with respect to recently established credit relationships
 - d. An account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor
- B. Suspicious Documents
 5. Documents provided for identification appear to have been altered or forged

6. The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification
7. Other information on the identification is not consistent with information provided by the person opening a new covered account or customer presenting the identification
8. Other information on the identification is not consistent with readily accessible information that is on file with the Department, such as a signature card or a recent check
9. An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

C. Suspicious Personal Identifying Information

10. Personal identifying information provided is inconsistent when compared against external information sources used by the Department. For example:
 - a. The address does not match any address in the consumer report
 - b. The Social Security Number (SSN) has not been issued, or is listed on the Social Security Administration's Death Master File
11. 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 death.
12. Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the Department. For example:
 - a. The address on an application is the same as the address provided on a fraudulent application
 - b. The telephone number on an application is the same as the number provided on a fraudulent application
13. Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the Department. For example:
 - a. The address on an application is fictitious, a mail drop, or a prison

- b. The phone number is invalid, or is associated with a pager or answering service
- 14. The SSN provided is the same as that submitted by other persons opening an account or other customers
- 15. 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 other persons opening account or other customers
- 16. The person opening the covered account or the customer fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete
- 17. Personal identifying information provided is not consistent with personal identifying information that is on file with the Department
- 18. If the Department uses challenge questions, the person opening the covered account or the customer cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report

The following shall be considered Red Flags in the case of already existing accounts.

D. Suspicious Account Activity or Unusual Use of Account

- 19. Shortly following the notice of a change of address for a covered account, the Department receives a request for a new, additional, or replacement account number, or for the addition of authorized users on the account
- 20. A new revolving credit account is used in a manner commonly associated with known patterns of fraud patterns. For example:
 - a. The customer fails to make the first payment or makes an initial payment but no subsequent payments
- 21. A covered account is used in a manner that is not consistent with established pattern of activity on the account. There is, for example:
 - a. Nonpayment when there is no history of late or missed payments
 - b. A material increase in the use of available credit
 - c. A material change in purchasing or spending patterns

22. A covered account 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)
 23. Mail sent to the account holder is repeatedly returned as undeliverable although transactions continue to be conducted in connection with the customer's covered account
 24. The Department is notified that the customer is not receiving mail sent by the Department
 25. The Department is notified of unauthorized charges or transactions in connection with a customer's covered account
- E. Alerts from Others Regarding Possible Identity Theft in Connection with Covered Accounts
26. The Department 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.

Detecting Red Flags

A. New Accounts

In order to detect any of the Red Flags identified above associated with the opening of a new account, staff shall take the following steps to obtain and verify the identity of the person opening the account:

1. Obtain identifying information about, and verify the identity of, a person opening a covered account, by utilizing such identifying information as the full name, date of birth, residential or business address, social security number, driver's license number, State issued Identification Card, passport, Alien Registration Receipt Card, or Consular Identification Card (CID) for individuals, and for businesses, the full entity name, principal place of business, local office, or physical location, and taxpayer identification number.
2. Verify the customer's identity for example, by reviewing a driver's license or other identification card for an individual, and reviewing documentation showing the existence of a business entity
3. Independently contact the prospective customer.

B. Existing Accounts

In order to detect any of the Red Flags identified above for an existing account, Department personnel shall take the following steps to monitor transactions with an account:

1. If a customer requests information about their account, either in person or by telephone, facsimile, or email, verify the identification of the customer
2. Verify the validity of requests to change billing addresses
3. Verify changes in banking information given for billing and payment purposes.

Preventing and Mitigating Identity Theft

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

1. Continue to monitor an account for evidence of Identity Theft
2. Contact the customer
3. Change any passwords or other security devices that permit access to accounts
4. Not open a new account
5. Close an existing account
6. Reopen an account with a new number
7. Notify the Program Administrator for determination of the appropriate step(s) to take
8. Notify the Criminal Investigations Bureau of the Police Department
9. Not attempt to collect on a covered account
10. Determine that no response is warranted under the particular circumstances.

Protecting customer identifying information

In order to further prevent the likelihood of identity theft occurring with respect to Departmental accounts, the Departments will take the following steps with respect to internal operating procedures, in order to protect customer identifying information:

1. Comply with Civil Code Section 1798.24 through 1798.24b, as applicable
2. Ensure that Departmental websites are secure or provide clear notice that they are not secure
3. Ensure that office computers are password protected and that computer screens lock after a set period of time
4. Ensure computer virus protection is up to date

5. Maintain paper based customer information in locked filing cabinets
6. Remove customer information from secured filing cabinets only as necessary and return it when no longer needed
7. Keep desks and work areas clear of papers containing customer information, including credit card information
8. Require and keep only the kinds of customer information that are necessary for Departmental business purposes
9. Ensure complete and secure destruction of paper documents and computer files containing customer information when no longer needed, in accordance with the City's Records Retention Schedule.

Program Updates

This Program shall be reviewed annually and updated as necessary to reflect changes in risks to customers and the City from the crime of Identity Theft. The Red Flag Task Force shall consider the City's experiences with Identity Theft, changes in Identity Theft methods, changes in Identity Theft detection and prevention methods, changes in the types of accounts the City maintains and changes in the City's business arrangements with third party service agencies. After considering these factors, the Red Flag Task Force shall recommend any necessary changes to the City Manager. Council approval shall be sought where required by law.

Program Administration

A. Oversight

Responsibility for developing, implementing and updating this Program lies with the Red Flag Administrator, in combination with each Department's Red Flag Officer. The Program Administrator shall be responsible for the overall administration of the Program, including ensuring appropriate training of City staff in recognizing Red Flags, reviewing any staff reports regarding the detection of Red Flags, preparing the Annual Red Flag Report, determining the prevention and mitigation action that should be taken in particular circumstances, and recommending periodic changes to the Program as necessary.

B. Staff Training and Reports

Each Department that maintains covered accounts shall ensure that staff assigned to service those accounts shall be trained by the Department to recognize the type of identifying information utilized by their Department to open new accounts. In addition, staff will also be trained to participate in the Red Flag Program, covering the opening of new accounts and the monitoring of existing accounts. Red Flag Training shall be provided by the Police Department Criminal Investigations Bureau at least annually.

Red Flag Officers for each Department shall be responsible for preparing any reports of Identity Theft for submission to the Program Administrator and the Red Flag Task Force.

C. Service Provider Agreements

As of May 1, 2009, the Red Flag Administrator shall be responsible for consulting with the Purchasing Division and the City Attorney's Office to develop a contractual requirement for service providers who have access to City covered accounts to maintain reasonable policies and procedures designed to detect, prevent, and mitigate the risk of Identity Theft of those accounts, and/or to comply with this Program in some other fashion acceptable to the City.

D. Specific Program Elements and Confidentiality

The success and effectiveness of the City's Red Flag Program depend to a large extent on confidentiality with respect to the City's specific practices relating to Identity Theft prevention. Therefore, under this Program, knowledge of specific practices is to be limited to the Program Administrator, officers, and those employees who need to know them for purposes of preventing Identity Theft. Because this Program is to be adopted by the City Council and is thus publicly available, it would be counterproductive to list these specific practices here. Therefore, only the Program's general Red Flag identification, detection, prevention, and mitigation procedures are listed in this document.

E. Legal and Regulatory Conformity

This Program shall be deemed modified to conform with changes in controlling law, as may be promulgated from time to time.