THE CITY OF SAN DIEGO

REPORT TO THE CITY COUNCIL

DATE ISSUED June 9, 2010 REPORT NO. 10-081

ATTENTION: Rules, Open Government, and Intergovernmental Relations Committee
Agenda of June 16, 2010

SUBJECT: Identity Theft Prevention Program

REQUESTED ACTION:

Approve the attached citywide Identity Theft Prevention Program policy as required by the Red Flags Rule of the Fair and Accurate Credit Transaction Act.

STAFF RECOMMENDATION:

Approve the Program policy.

SUMMARY:

A report of the President's Identity Theft Task Force indicates that identity theft, (a fraud attempted or committed using identifying information of another person without authority), results in billions of dollars in losses each year to individuals and businesses. To address this, the Federal Trade Commission (FTC), the federal bank regulatory agencies and the National Credit Union Administration (NCUA) issued regulations requiring financial institutions and creditors to develop and implement written identity theft prevention programs as part of the Fair and Accurate Credit Transaction (FACT) Act of 2003. These regulations are known as the Red Flags Rules. The Red Flags Rules apply to "financial institutions" and "creditors" with "covered accounts."

DISCUSSION:

The final Red Flags Rules require each financial institution and creditor that holds any consumer account, or other account for which there is a reasonably foreseeable risk of identity theft, to develop and implement an Identity Theft Prevention Program (Program) for combating identity theft in connection with new and existing accounts. Under the Rules, the definition of "creditor" is broad, and includes businesses or organizations that regularly provide goods or services first and allow customers to pay later. The Rules apply to government agencies if the activities of the government agency fall within the statutory definitions of "financial institution" or "creditor."

For example, cities that operate utilities that regularly bill customers after they've received services are creditors under the Rules. The City of San Diego is considered a creditor and therefore prepared the attached citywide Identity Theft Prevention Program policy.

As required, this policy requires impacted departments to develop specific procedures for detecting, preventing, and mitigating identity theft and enables the City to:

1. Identify relevant patterns, practices, and specific forms of activity that are "red flags" signaling possible identity theft and incorporate those red flags into the Program;
2. Detect red flags that have been incorporated into the 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 from identity theft.

Individual Departments (i.e. Utilities, City Treasurer, Police, etc.) have either developed or are in process of developing specific procedures related to their activities. Responsibility for developing, implementing, and updating the Program policy lies with the Administration Department Director and the designated Identity Theft Prevention Committee. The Committee is comprised of representatives of Human Resources, Information Technology, Purchasing & Contracting, Parks and Recreation, Development Services, Public Utilities, Police and City Treasurer.

The Program policy will be periodically reviewed and updated to reflect changes in risks to individuals and the soundness of the City's Program to protect individuals from identity theft. At least annually, we will consider our experiences with identity theft situations, changes in identity theft methods, changes in identity theft detection and prevention methods, changes in types of accounts it maintains, and changes in the City's business arrangements with other entities. After considering these factors, the Program Committee will determine whether changes to the Program, including the listing of Red Flags, are warranted. If warranted, the Program Committee will recommend updates to the Program, pending management approval.

FISCAL IMPACT:

Existing staff will implement the Program policy and prepare process narratives as appropriate. We anticipate the fiscal impact to be minimal.

Debra Fischle-Faulk

Debra Fischle-Faulk, Director
Administration Department

Approved: Wally Hill

Wally Hill
Assistant Chief Operating Officer

Attachment: Citywide Identity Theft Prevention Program

City of San Diego
Identity Theft Prevention Program Policy

I. POLICY

It is the City of San Diego's policy to protect our customers and their accounts from identity theft and to comply with the Federal Trade Commission's (FTC) Red Flags Rule. This will be accomplished by developing and implementing this written Identity Theft Prevention Program Policy (Program), which is appropriate to our size, complexity, and the nature and scope of our activities. This Program addresses the City's requirement to: 1) identify relevant identity theft Red Flags, 2) detect those Red Flags, 3) respond appropriately to any that are detected to prevent and mitigate identity theft, 4) update our Program periodically to reflect changes in risks and 5) include a process for administration and oversight of the program.

Based on definitions included in the Red Flags Rules, this Program at minimum applies to the Public Utilities, Police, City Treasurer and Development Services Departments. This Program may also apply to other business functions of the City in the future.

II. DEFINITIONS

Account: a continuing relationship with a creditor to obtain a product or service that includes deferred payments for services or property.

Covered account: (1) an account offered or maintained by the City primarily for personal, business and household purposes that involves or is designed to permit multiple payments or transactions; and (2) any other account offered or maintained by the City for which identity theft is a reasonably foreseeable risk that may impact the City's customers or the safety and soundness of the City, including financial, operational, compliance, reputation, or litigation risks. An example of a City of San Diego "covered account" is a customer billing account (i.e. utility bill). Because a customer does not arrange or voluntarily enter into the transaction and the relationship established is not for goods and services, the following accounts are not considered covered accounts:

Taxes
Parking citations
Fines imposed

If the covered account is provisioned by or processed by a third party, then the guidance regarding third parties may apply (see Section VI).

Credit: the right granted by a creditor to a debtor to defer payment of debt or to incur debt and defer its payment or to purchase property or services and defer payment therefore.

Creditor: any person or business who arranges for the extension, renewal, or continuation of credit with a covered account.

Identity Theft: fraud committed or attempted using the identifying information of another person without authority.

Identifying Information: any name or number that may be used, alone or in conjunction 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.

Red Flag: a pattern, practice, or specific activity that indicates the possible existence of identity theft.

III. IDENTIFICATION OF RED FLAGS

To identify relevant Red Flags, appropriate City Departments must assess the following risk factors: 1) types of covered accounts offered, 2) methods provided to open or access these accounts, and 3) previous experience with identity theft, if applicable. Red Flags are considered from the following five categories (and the 26 numbered examples under them) as they fit our situation:

A. Alerts, Notifications, and Warnings From a Credit Reporting Company

Red Flags

1. Report of fraud accompanying a credit report;
2. Notice or report from a credit agency of a credit freeze on an individual;
3. Notice or report from a credit agency of an active duty alert for an individual;
4. Receipt of a notice of address discrepancy in response to a credit report request; and
5. Indication from a credit report of activity that is inconsistent with an individual's usual pattern or activity.

B. Suspicious Documents

Red Flags

6. Identification document or card that appears to be forged, altered, or inauthentic;
7. Identification document or card on which a person's photograph or physical description is not consistent with the person presenting the document;
8. Other documents with information that is not consistent with existing personal information (such as if a person's signature does not match between different documents, or does not match signature on file); and
9. Application that appears to have been altered or forged.

C. Suspicious Personal Identifying Information

Red Flags

10. Identifying information presented that is inconsistent with other information the individual provides (example: inconsistent birth dates);
11. Identifying information presented that is inconsistent with other sources of information (for instance, an address not matching an address on a credit report);

12. Identifying information presented that is the same as information shown on other applications that were found to be fraudulent;
13. Identifying information presented that is consistent with fraudulent activity (such as an invalid phone number);
14. Social security number presented that is the same as one given by another individual;
15. An address or phone number presented that is the same as that of another person;
16. A person fails to provide complete personal identifying information on an application when reminded to do so;
17. A person's identifying information is not consistent with the information that is on file for the individual.

D. Suspicious Account Activity or Unusual Use of Account

Red Flags

18. Change of address for an account followed by a request to change the individual's name;
19. Payments stop on an otherwise consistently up-to-date account;
20. Account used in a way that is not consistent with prior use;
21. Mail sent to the account holder is repeatedly returned as undeliverable;
22. Notice to the City that the individual is not receiving mail sent by the firm;
23. Notice to the City that an account has unauthorized activity;
24. Breach in the city's computer system security; and
25. Unauthorized access to or use of individual account information.

E. Alerts From Others

Red Flag

26. Notice to the City from an individual, identity theft victim, law enforcement, or other person that it has opened or is maintaining a fraudulent account for a person engaged in identity theft.

Some of these categories and examples may not be relevant, and some may be relevant only when combined or considered with other indicators of identity theft. The examples are not exhaustive or a mandatory checklist, but a way to help departments think through relevant Red Flags in the context of the City's business. Based on this review of the risk factors, sources, and FTC examples of Red Flags, we have identified our Red Flags. Appropriate Departments will prepare process narratives as necessary.

IV. DETECTING RED FLAGS

A. New Accounts

In order to detect any of the Red Flags identified above associated with the opening of a **new covered account**, the appropriate City staff will take steps to obtain and verify the identity of the person opening the account. Each business unit responsible for offering covered accounts is expected to document the steps they will take, considering methods such as:

1. Requiring certain identifying information such as name, date of birth, address, driver's license, or other identification, and, where feasible, to compare with existing file information for the individual;

2. Verifying the identity (i.e. request the customer to appear in person with a government-issued photo ID card or another form of photo identification accompanied by a birth certificate or social security card); or

3. Independently contacting the purported individual, using contact information already on file in the City's systems.

B. Existing Accounts

In order to detect any of the Red Flags identified above for an **existing covered account**, appropriate City staff will take steps to monitor transactions with an account. Each business unit responsible for monitoring covered accounts is expected to document the steps they will take, considering methods such as:

1. If an individual is requesting information in person, or via telephone, fax, or email, then verifying the identification of the individual prior to providing the information;

2. Verifying the validity of requests to change billing addresses, and/or confirming changes, such as sending a change confirmation to email address on file; or

3. Verifying changes in banking information given for billing and payment purposes, such as contacting the individual via information already on file, prior to making any changes.

V. RESPONDING TO RED FLAGS TO MITIGATE IDENTITY THEFT

In the event City staff detects any identified Red Flags, such personnel shall take one or more of the following steps, after consulting with department management and depending on the degree of identity theft risk posed by the Red Flag:

A. Prevent and Mitigate

1. Contact the affected individual, using information already on file;
2. Change any passwords or other security devices that permit access to accounts;
3. Continue to monitor an account for evidence of identity theft;
4. Not open a new account;
5. Close an existing account;
6. Reopen an account with a new number;
7. Notify the Program Administrator to have the incident logged, and for additional assistance if needed;
8. Determine that no response is warranted under the particular circumstances.

B. Protect Personal Information

In order to further prevent the likelihood of identity theft occurring with respect to City accounts, City staff will adhere to the policies and practices regarding protection of personal information by:

1. Collecting only the personal information that is needed for our purposes;
2. Retaining personal information for only the time period legally required and/or necessary for our purposes;
3. Protecting personal information collected, used, disclosed, and retained;
4. Ensuring additional protection methods on sensitive personal information that is retained;
5. Restricting access to personal information only to individuals who have a business need to access information;
6. Disposing of personal information appropriately;
7. Instilling awareness and training employees on the proper handling of personal information;
8. Understanding the requirements of applicable data privacy protection laws and regulations;
9. Conducting regular risk assessments to identify where and how the City stores or transmits personal information;
10. Developing, reviewing, and assessing the information security management program, policies, and procedures to ensure they are current and effectively communicated throughout the City.

VI. PROGRAM ADMINISTRATION

A. Oversight

Responsibility for developing, implementing, and updating this Program policy lies with the Administration Department Director and the designated Identity Theft Prevention Committee. The Committee is comprised of representatives of Human Resources, Information Technology, Purchasing & Contracting, Development Services, Parks and Recreation, Public Utilities, Police and City Treasurer.

The Committee will be responsible for the Program administration, ensuring appropriate training of City staff on the Program, for reviewing any staff reports regarding the detection of Red Flags and the steps for preventing and mitigating identity theft, determining which steps of prevention and mitigation should be taken in particular circumstances, and considering periodic changes to the Program. The Committee will annually report to the Assistant Chief Operating Officer.

B. Program Updates

This Program policy will be periodically reviewed and updated to reflect changes in risks to individuals and the soundness of the City's Program to protect individuals from identity theft. At least annually, the City will consider applicable law and financial regulations, its experiences with identity theft situations, changes in identity theft methods, changes in identity theft detection and prevention methods, changes in types of accounts it maintains, and changes in the City's business arrangements with other entities. After considering these factors, the Program Committee will determine whether changes to the Program, including the listing of Red Flags, are warranted. If warranted, the Program Committee will recommend updates to the Program, pending management approval.

C. Staff Training and Reports

City staff responsible for implementing the Program shall be trained in the detection of Red Flags, and the responsive steps to be taken when a Red Flag is detected. The Human Resources Department will provide this training. Areas with covered accounts will review the Program at least annually, incorporating any Program updates in their processes. New employees are

expected to be trained prior to any involvement with covered accounts. Staff is expected to report any suspicious activity to the Program Administrator; this will automatically create a record in the reporting system. The Program Committee will prepare an annual review of the Program, including compliance and effectiveness.

D. Service Provider Arrangements

In the event the City engages a service provider to perform an activity in connection with one or more covered accounts, the City will take steps to ensure the service provider performs its activity in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft. This may include a review of the service provider's Red Flag Identity Theft Program, or contract language with regard to policies and procedures. Additionally, the City and the service provider should have a mutually agreeable means for notification in the event the service provider identifies a Red Flag situation.

VII. APPROVAL

I approve this Identity Theft Prevention Program as reasonably designed to enable the City to detect, prevent, and mitigate identity theft.

Wally Hill
Assistant Chief Operating Officer

6-1-10
Date