Policy 7.1.6 Customer Credit Security Program

POLICY PURPOSE:

The purpose of this policy is to comply with 16 CFR 681.2 (Fair & Accurate Credit Transaction Act of 2003) in order to detect, prevent and mitigate identity theft by identifying and detecting identity theft red flags and by responding to such red flags in a manner that will prevent identity theft for customers of the City of Sunnyvale. This policy applies to City employees, contractors, consultants, temporary workers and all personnel affiliated with third parties that perform work for the City.

POLICY STATEMENT:

1. Definitions

A. City

City means City of Sunnyvale.

B. Covered Account

(I.) An account that the City of Sunnyvale maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions, such as a utility account or a housing loan.

(II.) Any other account that the City or a third party offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the City from identity theft, including financial, operational, compliance, reputation, or litigation risks.

C. Credit

The right granted by the City to a debtor to defer payment of debt or to incur debts and defer its payment or to purchase property or services and defer payment therefore.

D. Creditor

Any entity that 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 the decision to extend, renew, or continue credit and includes utility companies and mortgage lenders.

E. Customer

A person that has a covered account with a creditor.

F. Identity Theft

A fraud committed or attempted using identifying information of another person without authority.

G. Person

A natural person, a corporation, government or governmental subdivision or agency, trust, estate, partnership, cooperative, or association.

H. Personal Identifying Information

Including but not limited to a person's credit card account information, debit card information, bank account information, drivers' license information and social security number.

I. Privacy Officer

That City employee designated by City's City Manager to administer City's Customer Credit Security Program.

J. Red flag

A pattern, practice, or specific activity that indicates the possible existence of identity theft.

K. Service provider

A person or entity that provides a service directly to the city

2. Findings

A. The City is a creditor due to its provision or maintenance of covered accounts for which payment is made in arrears and must develop and implement a written Identity Theft Prevention Program that is designed to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account.

B. Covered accounts offered to customers for the provision of city services include but are not limited to water, wastewater, garbage collection, home loans, and other accounts for services held by the City.

C. The process of opening a new covered account, restoring an existing covered account, making payments on such accounts, and transferring services have been identified as potential processes in which identity theft could occur.

D. The City limits access to personal identifying information to those employees responsible for or otherwise involved in opening or restoring covered accounts or accepting payment for use of covered accounts.

E. The City determines that there is a low risk of identity theft occurring in the following ways:

(I.) Use of an applicant of another person's personal identifying information to establish a new covered account.

(II.) Use of a previous customer's personal identifying information by another person in an effort to have service restored in the previous customer's name.

(III.) Use of another person's credit card, bank account, or other method of payment by a customer to pay such customer's covered account or accounts.

(IV.) Use by a customer desiring to restore such customer's covered account of another person's credit card, bank account or other method of payment.

3. Process of Establishing a Covered Account

A. A precondition to opening a covered account for City services, each applicant shall provide personal identifying information as identified by the standard operating procedure of the department administering the covered account.

4. Access to Covered Account Information

A. Access to customer accounts shall be limited to authorized City personnel.

B. Any unauthorized access to or other breach of customer accounts is to be reported immediately to the Privacy Officer or designee.

C. Personal identifying information included in customer accounts is considered confidential and any request or demand for such information by someone other than the verified customer shall be immediately forwarded to the Privacy Officer or designee.

5. Sources and Types of Red Flags

All City employees responsible for or involved in the process of opening a covered account, restoring a covered account or accepting payment for a covered account shall check for red flags as indicators of possible identity theft and such red flags may include:

A. Alerts from consumer reporting agencies, fraud detection agencies or service providers. Examples of alerts include but are not limited to:

(I.) A fraud or active duty alert that is included with a consumer report;

(II.) A notice of credit freeze in response to a request for a consumer report;

(III.) A notice of address discrepancy provided by a consumer reporting agency;

(IV.) Indications of a pattern of activity in a consumer report that is inconsistent with the history and usual pattern of activity of an applicant or customer, such as 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. Examples of suspicious documents include:

(I.) Documents provided for identification that appear to be altered or forged;

(II.) Photograph or physical description on Identification is inconsistent with the appearance of the applicant or customer;

(III.) Information on Identification is inconsistent with information provided by the applicant or customer;

(IV.) Identification on which the information is inconsistent with readily accessible information that is on file with the financial institution or creditor, such as a signature card or a recent check; or

(V.) An application that appears to have been altered or forged, or appears to have been destroyed and reassembled.

C. Suspicious personal identification, such as suspicious address change. Examples of suspicious identifying information include:

(I.) Personal identifying information that is inconsistent with external information sources used by the financial institution or creditor. 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.

(II.) Personal identifying information provided by the customer is not consistent with other personal identifying information provided by the customer.

(III.) Personal identifying information or a phone number or address, is associated with known fraudulent applications or activities as indicated by internal or third-party sources used by the financial institution or creditor.

(IV.) Other information provided, such as fictitious mailing address, mail drop addresses, jail addresses, invalid phone numbers, pager numbers or answering services, is associated with fraudulent activity.

(V.) The SSN provided is the same as that submitted by other applicants or customers.

(VI.) 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 applicants or customers.

(VII.) The applicant or customer fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete.

(VIII.) Personal identifying information is not consistent with personal identifying information that is on file with the financial institution or creditor.

(IX.) The applicant or 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 relating to a covered account. Examples of suspicious activity include:

(I.) Shortly following the notice of a change of address for an account, city receives a request for the addition of authorized users on the account.

(II.) An account is used in a manner that is not consistent with established patterns of activity on the account. There is, for example, a material change in payment patterns;

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

(IV.) City is notified that the customer is not receiving paper account statements.

(V.) City is notified of unauthorized charges or transactions in connection with a customer's account.

(VI.) City is notified by a customer, law enforcement or another person that it has opened a fraudulent account for a person engaged in identity theft.

E. Notice from customers, law enforcement, victims or other reliable sources regarding possible identity theft or phishing relating to covered accounts.

6. Prevention and Mitigation of Identity Theft

A. In the event that any City employee responsible for or involved in restoring an existing covered account or accepting payment for a covered account becomes aware of red flags indicating possible identity theft with respect to existing covered accounts, such employee shall use his or her discretion to determine whether such red flag or combination of red flags suggests a threat of identity theft. If, in his or her discretion, such employee determines that identity theft or attempted identity theft is likely or probable, such employee shall immediately report such red flags to the Privacy Officer or designee. If, in his/her discretion, such employee deems that identity theft is unlikely or that reliable information is available to reconcile red flags, the employee shall convey this information to the Privacy Officer, who may in his/her discretion determine that no further action is necessary. If the Privacy Officer determines that further action is necessary, a City employee shall perform one or more of the following responses, as determined to be appropriate:

(I.) Contact the customer;

(II.) Make changes to the account if, after contacting the customer, it is apparent that someone other than the customer has accessed the customer's covered account. Changes may include but are not limited to changing any account numbers, passwords, security

codes, or other security devices that permit access to an account; or closing the account;

(III.) Cease attempts to collect additional charges from the customer and decline to submit the customer's account to a debt collector in the event that the customer's account has been accessed without authorization and such access has caused additional charges to accrue;

(IV.) Notify a debt collector within two business days of the discovery of likely or probable identity theft relating to a customer account that has been provided to such debt collector in the event that a customer's account has been submitted to a debt collector prior to the discovery of the likelihood or probability of identity theft relating to such account;

(V.) Notify law enforcement, in the event that someone other than the customer has accessed the customer's account causing additional charges to accrue or accessing personal identifying information; or

(VI.) Take other appropriate action to prevent or mitigate identity theft.

B. In the event that any City employee responsible for or involved in opening a new covered account becomes aware of red flags indicating possible identity theft with respect an application for a new account, such employee shall use his or her discretion to determine whether such red flag or combination of red flags suggests a threat of identity theft. If, in his or her discretion, such employee determines that identity theft or attempted identity theft is likely or probable, such employee shall immediately report such red flags to the Privacy Officer or designee. If, in his/her discretion, such employee deems that identity theft is unlikely or that reliable information is available to reconcile red flags, the employee shall convey this information to the Privacy Officer, who may in his/her discretion determine that no further action is necessary. If the Privacy Officer or his/her designee in his/her discretion determines that further action is necessary, a City employee shall perform one or more of the following responses, as determined to be appropriate:

(I.) Request additional identifying information from the applicant;

(II.) Deny the application for the new account;

(III.) Notify law enforcement of possible identity theft; or
(IV.) Take other appropriate action to prevent or mitigate identity theft.

7. Duties Regarding Addressing Discrepancies

A. City departments which use credit reports shall develop standard operating procedures designed to enable the department to form a reasonable belief that a credit report relates to the consumer for whom it was requested if the department receives a notice of address discrepancy from a nationwide consumer reporting agency indicating the address given by the consumer differs from the address contained in the consumer report.

B. A City employee responsible for confirming that an address is accurate may do so by any of the following means:

(I.) Verification of the address with the consumer;

(II.) Review of the utility's records;

(III.) Verification of the address through third-party sources; or

(IV.) Other reasonable means.

C. If an accurate address is confirmed, the responsible employee shall furnish the consumer's address to the nationwide consumer reporting agency from which it received the notice of address discrepancy if:

(I.) The City establishes a continuing relationship with the consumer; and

(II.) The City, regularly and in the ordinary course of business, furnishes information to the consumer reporting agency.

8. Updating this Program

A. The City Manager or designee shall annually review and, as deemed necessary, update this Program along with any relevant red flags in order to reflect changes in risks to customers or to the safety and soundness of City and its covered accounts from identity theft.

9. Program Administration

A. The Privacy Officer is responsible for oversight of this Program and for Program implementation and is responsible for reviewing reports prepared by City staff regarding compliance with red flag requirements and with recommending material changes to the Program, as necessary in the opinion of the City Manager or City Attorney to address changing identity theft risks and to identify new or discontinued types of covered accounts. Any

recommended material changes to the program shall be submitted to the City Council for consideration and approval.

B. The Privacy Officer will request from each department at least annually, a statement of compliance with the red flag requirements. The report will address material matters related to this Program and evaluate issues such as:

(I.) The effectiveness of the policies and procedures of City in addressing the risk of identity theft in connection with the opening of covered accounts and with respect to existing covered accounts;

(II.) Service provider arrangements;

(III.) Significant incidents involving identity theft and management's response; and

(IV.) Recommendations for material changes to the Program.

C. The Privacy Officer or designee is responsible for providing training to all employees responsible for or involved in opening a new covered account, restoring an existing covered account or accepting payment for a covered account with respect to the implementation and requirements of this Program. The Privacy Officer shall exercise their discretion in determining the amount and substance of training necessary.

10. Outside Service Providers

A. In the event that City engages a service provider to perform an activity in connection with one or more covered accounts the Privacy Officer shall exercise their discretion in reviewing such arrangements in order to ensure, to the best of their ability, that the service provider's activities are conducted in accordance with policies and procedures, agreed upon by contract, that are designed to detect any red flags that may arise in the performance of the service provider's activities and take appropriate steps to prevent or mitigate identity theft.

(Adopted: RTC # 09-105 (4/28/09))

Lead Department: Department of Finance