



Memorandum

TO: HONORABLE MAYOR AND
CITY COUNCIL

FROM: Debra Figone,
City Manager

**SUBJECT: FAIR AND ACCURATE CREDIT
TRANSACTIONS ACT OF 2003,
IDENTITY THEFT PREVENTION
PROGRAM**

DATE: October 15, 2008

RECOMMENDATION

It is recommended that the City Council adopt a resolution approving the Identity Theft Prevention Program and Procedures Related to Notices of Address Discrepancies to comply with regulations issued by the Federal Trade Commission pursuant to the Fair and Accurate Credit Transactions Act of 2003 and designation of the City Manager's Office to provide oversight of the Identity Theft Prevention Program.

OUTCOME

Upon approval of the Identity Theft Prevention Program (ITPP) and Procedures Related to Notices of Address Discrepancies, the City of San Jose will be compliant with regulations issued by the Federal Trade Commission pursuant to the Fair and Accurate Credit Transactions (FACT) Act of 2003.

BACKGROUND

The Federal Trade Commission issued regulations which require creditors with "covered accounts" to design and implement a written identity theft prevention program by November 1, 2008. Similar regulations, which require banks and credit unions to implement a written identity theft prevention program by November 1, 2008, were adopted by federal banking agencies and the National Credit Union Administration. The FTC Regulations, also known as the "Red Flag Rules," require that the initial program be approved by the City Council. The FTC has the

HONORABLE MAYOR AND CITY COUNCIL

October 15, 2008

Subject: Identity Theft Prevention Program

Page 2

authority to enforce compliance with the regulations through civil actions to impose penalties. The California Attorney General also has authority to take enforcement action.

The City has determined that it is a creditor with "covered accounts" under the FTC Regulations and, consequently, is required to have an Identity Theft Prevention Program in place because the City provides water, sewer, and solid waste services for which payment is made after the service is consumed or the service has otherwise been provided. The City also offers, or has outstanding loans, for the following purposes: (1) home rehabilitation; (2) home purchase; (3) teacher education; and (4) small business loan programs. These loan accounts are also covered accounts under the FTC Regulations in that there is a foreseeable, albeit low risk, of identity theft in the opening or maintenance of these loans.

The Federal Trade Commission also has issued regulations that require users of consumer credit reports to develop policies and procedures relating to address discrepancies between information provided by a consumer and information provided by a consumer reporting agency. The City uses consumer credit reports in connection with various loan programs, debt collection and the hiring process. The procedures related to notices of address discrepancies sent to the City by a consumer reporting agency are included in the same document as the Identity Theft Prevention Program for ease of reference.

ANALYSIS

The proposed Identity Theft Prevention Program and the Procedures related to Notices of Address Discrepancies is attached to this memorandum. Set forth below is a brief overview of the Program.

Elements of Program

The FTC Regulations provide that the Identity Theft Prevention Program must include the following elements: (1) identify relevant patterns, practices or activities that are indicative of identity theft, i.e., "Red Flags"; (2) detect the Red Flags that have been incorporated in the program; (3) provide for appropriate responses to the identified Red Flags when they occur in order to prevent or mitigate identity theft with respect to the covered accounts; and (4) set forth a plan to update the program at least annually.

Risk Assessment

The FTC Regulations require that the City conduct a risk assessment to determine whether the accounts it offers or maintains are subject to a reasonably foreseeable risk of identify theft, whether that risk is to the customers or to the creditor itself.

The City has determined that there is a low risk of identity theft occurring in the following ways:

- a. Use by an applicant of another person's personal identifying information to establish a new covered account;
- b. 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;
- c. 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; and
- d. 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.

Staff has reviewed the process of establishing a covered utility account in which applicants provide the City with personal identifying information such as a driver's license number, the last four digits of their social security number, and/or date of birth and determined that there is a low risk associated with identity theft in regards to this information. Access to account information is limited to authorized personnel. As a precautionary measure, receipts for utility accounts paid by credit cards are masked except for the last four digits of the account number. In addition, transactions handled by Kubra, the City's payment vendor for the covered utility accounts, follow strict data security measures and the City's contract with the vendor requires the vendor to keep its security practices current by performing third party audits.

The City also has various loan programs for individuals and sole proprietorships. All of these programs involve the collection and maintenance of personal identifying information of the loan recipients. The Housing Department offers the following loan programs: Housing Rehabilitation, Teacher Homebuyer, San Jose State University Faculty and Staff Homebuyer, and Equity-Share Homebuyer. The Parks Recreation and Neighborhood Services Department and the Office of Economic Development are currently overseeing the existing Future Teacher and Small Business loan program accounts, respectively as new loans are not being offered under either of these programs. As described in the proposed Program, the risk of identify theft occurring in the opening of these loan accounts and in the maintenance of these accounts is low.

Furthermore, the City has taken a proactive role in assessing the security risks that may arise with its information systems. In July 2008, the Information Technology Department performed an audit of key department and systems to enhance data security and privacy. In addition to the security audit, the IT Department has hired a consultant to enhance the City's security posture as it relates to information.

Sources and Types of Red Flags

The FTC Regulations identify possible Red Flags which a creditor should consider in developing its Identity Theft Prevention Program. These fall into five categories: (1) alerts, notifications, or

other warnings received from consumer reporting agencies or service providers; (2) presentation of suspicious documents; (3) presentation of suspicious personal identifying information; (4) unusual use of, or other suspicious activity related to, an account; and (5) notice from customers, victims of identity theft, or law enforcement activities. Not all of the Red Flags listed in the FTC Regulations are applicable to the City's covered accounts. The listing of Red Flags in the regulations also apply to deposit accounts offered by financial institutions and service accounts offered by cell phone companies where there is a greater risk of identity theft. Staff has reviewed the Red Flags and has identified those that are relevant to the City's covered accounts.

Detection and Response to Red Flags

All 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. The ITTP Program identifies the measures that should be taken by staff in response to the identification of a Red Flag. These steps include notification, as appropriate, to the customer, supervisory staff within the department with oversight of the covered account, the City Manager's Office, City Attorney's Office and/or the San José Police Department.

Program Administration and Annual Update

The City Manager's Office (CMO), or designee, will annually review and update the ITTP along with any relevant Red Flags in order to reflect changes in risks to customers or to the safety and soundness of the City and its covered accounts from identity theft. In so doing, the CMO will consider the following factors and exercise its discretion in amending the program:

- (1) The City's experiences with identity theft;
- (2) Updates in methods of identity theft;
- (3) Updates in customary methods used to detect, prevent, and mitigate identity theft;
- (4) Updates in the types of accounts that the City offers or maintains; and
- (5) Updates in service provider arrangements.

EVALUATION AND FOLLOW-UP

Senior Level Staff within the stakeholder departments are responsible for oversight of the program and for program implementation. The City Manager is responsible for reviewing annual reports prepared by staff regarding compliance with red flag requirements addressing changing identity theft risks and identifying new or discontinued types of covered accounts and determining which changes to the program are material. Any recommended material changes to the program, as determined by the City Manager, will be submitted to the City Council for consideration.

POLICY ALTERNATIVES

NA

PUBLIC OUTREACH/INTEREST

- Criteria 1:** Requires Council action on the use of public funds equal to \$1 million or greater. **(Required: Website Posting)**

- Criteria 2:** Adoption of a new or revised policy that may have implications for public health, safety, quality of life, or financial/economic vitality of the City. **(Required: E-mail and Website Posting)**

- Criteria 3:** Consideration of proposed changes to service delivery, programs, staffing that may have impacts to community services and have been identified by staff, Council or a Community group that requires special outreach. **(Required: E-mail, Website Posting, Community Meetings, Notice in appropriate newspapers)**

COORDINATION

This memorandum has been coordinated with the Finance Department, Housing Department, the Information Technology Department, the Office of Economic Development, the Parks Recreation and Neighborhood Services Department, Human Resources / Risk Management Department, and the City Attorney's Office.

COST SUMMARY/IMPLICATIONS

Any operating costs associated with the proposed program will be included in the City's operating budget. Any capital costs associated with implementing changes to the utility billing program will be included in the appropriate budget.

HONORABLE MAYOR AND CITY COUNCIL
October 15, 2008
Subject: Identity Theft Prevention Program
Page 6

BUDGET REFERENCE

N/A

CEQA

Not a project.

Christine J. Shippey

for

Debra Figone
City Manager
City of San Jose

Attachment

ATTACHMENT A



**CITY OF SAN JOSE
IDENTITY THEFT PREVENTION PROGRAM
(ITPP)
And
PROCEDURES RELATED TO NOTICES OF
ADDRESS DISCREPANCIES**

In Accordance with the Fair and Accurate Credit Transactions Act of 2003

And

16 CFR § 681.1 and 16 CFR §681.2

Approved by the City Council October XX, 2008. Updated: October XX, 2008

**CITY OF SAN JOSE
IDENTITY THEFT PREVENTION PROGRAM**

Purpose

The purpose of the Identity Theft Prevention Program (“ITPP” or “Program”) is to comply with the Federal Trade Commission regulations issued under the Fair and Accurate Credit Transactions (FACT) Act of 2003. The Program will assist staff 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 and mitigate identity theft.

Background

The Federal Trade Commission regulations governing the Identity Theft Prevention Program, adopted as 16 CFR § 681.2 (referred to as the “FTC Regulations”), require creditors, to develop and provide a written program to detect, prevent and mitigate identity theft in connection with the opening of a covered account or any existing covered account. Under the FTC Regulations, “creditor” is a person that extends, renews or continues credit, and defines “credit”, in part, as the right to purchase property or services and defer payment therefore. The FTC Regulations include utility companies in the definition of creditor.

The FTC Regulations define “covered account”, in part, as an account that a creditor provides for personal, family or household purposes that is designed to allow multiple payments or transactions or any other account that the creditor maintains for which there is a foreseeable risk to customers or to the safety and soundness of the creditor from identity theft. The FTC Regulations specify that a utility account is a covered account.

The City has determined that it is a creditor under the FTC Regulations and consequently is required to have an Identity Theft Prevention Program in place because the City provides water, sewer, and solid waste services for which payment is made after the service is consumed or the service has otherwise been provided. The City also has loan programs in which credit is extended to individuals or sole proprietorships for the following purposes: (1) home rehabilitation; (2) home purchase; (3) teacher education; and (4) small business loan programs.

The FTC Regulations specify guidelines that should be considered in the development of the Program, taking into account the past incidents of identity theft with respect to the City’s covered accounts and the City’s assessment of the risk of future incidents.

Accordingly, the City's Program provides a basic framework governing the City's policies and procedures for the identification, prevention and mitigation of incidents of identity theft with respect to the City's covered accounts. In developing the Program, the City has considered relevant "red flags" outlined in the FTC Regulations which are patterns, practices, or specific activities that indicate the possible existence of identity theft with respect to a covered account.

Consistent with the FTC Regulations, the initial Program is to be in place by November 1, 2008 and requires City Council approval. The implementation and administration of the Program is to be overseen by the City Manager's Office.

The Federal Trade Commission also has issued regulations, adopted as 16 CFR § 681.1, to require users of consumer credit reports to develop policies and procedures relating to notices regarding address discrepancies from a consumer reporting agency. The City uses consumer credit reports for a variety of purposes such as: obtaining credit information regarding loan applicants; locating delinquent debtors; and conducting background checks in the City's hiring process.

Definitions

The following definitions apply to the Identity Theft Prevention Program (ITPP).

- (a) "Covered account" means (i) An account that a financial institution or creditor offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions, such as a credit card account, mortgage loan, automobile loan, margin account, cell phone account, utility account, checking account, or savings account; and (ii) Any other account that the financial institution or creditor offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the financial institution or creditor from identity theft, including financial, operational, compliance, reputation, or litigation risks.
- (b) "Credit" means the right granted by a creditor 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.
- (c) "Creditor" means 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 the decision to extend, renew, or continue credit and includes utility companies and telecommunications companies.
- (d) "Customer" means a person that has a covered account with a creditor.

- (e) "Identity theft" means a fraud committed or attempted using identifying information of another person without authority.
- (f) "Loan Programs" mean the following City loan programs: Housing Rehabilitation, Teacher Homebuyer, SJSU Faculty and Staff Homebuyer, Equity-Share Homebuyer, Future Teacher and Small Business.
- (g) "Personal 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:
 - (i) Name, 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;
 - (ii) Unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation.
 - (iii) Unique electronic identification number address or routing code.
 - (iv) Telecommunication identifying information or access device as defined in 18 U.S.C.1029(e), which states: any card, plate, code, account number, electronic serial number, mobile identification number, personal identification number, or other telecommunications service, equipment, or instrument identifier, or other means of account access that can be used, alone or in conjunction with another access device, to obtain money, goods, services, or any other thing of value, or that can be used to initiate a transfer of funds (other than a transfer originated solely by paper instrument); means any card, plate, code, account number, electronic serial number, mobile identification number, personal identification number, or other telecommunications service, equipment, or instrument identifier, or other means of account access that can be used, alone or in conjunction with another access device, to obtain money, goods, services, or any other thing of value, or that can be used to initiate a transfer of funds (other than a transfer originated solely by paper instrument).
- (h) "Red flag" means a pattern, practice, or specific activity that indicates the possible existence of identity theft.
- (i) "Service provider" means a person that provides a service directly to the City.
- (j) "Stakeholder Department" means a City department responsible for the oversight of a covered account.

Risk Assessment

- (1) The City is a creditor due to its provision or maintenance of covered accounts for which payment is made in arrears and as a lender in the Loan Programs.
- (2) Covered accounts are offered to customers for the provision of City water, sewer, solid waste, and the loans issued under the Loan Programs.
- (3) The City has not encountered any reported incidents related to identity theft involving the City's covered accounts.
- (4) The processes of opening a new covered utility account, restoring an existing covered utility account and making payments on such accounts, have been identified as potential processes in which identity theft could occur.
- (5) 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.
- (6) The City determines that there is a low risk of identity theft occurring in utility accounts in the following ways:
 - a. Use by an applicant of another person's personal identifying information to establish a new covered account;
 - b. 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;
 - c. 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; and
 - d. 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.
- (7) The City determines that there is a low risk of identity theft occurring with the opening of a new covered account and with maintaining an existing covered account within the Loan Programs.

Process of Establishing a Covered Account

- (1) Covered Accounts for Utility Services. As a precondition to opening a utility account in the City, each applicant is requested to provide the City with personal identifying information such as driver's license number or Department of Motor Vehicles issued identification number, last four digits of the customer's social security number, and/or date of birth.

- (2) Covered Accounts for Loan Programs. The type of information required to determine eligibility for a loan varies depending on the type of loan as described below.
- a. Applicants for loans involving real property administered by the Housing Department. These applicants must provide: personal identification including Social Security Number and Driver's License Number, information that is necessary for obtaining a credit report, verification of title on the subject property, income tax returns, paycheck stubs, bank statements, property tax bill, and hazard insurance policy. All documents are compared for consistency in support of applicant ownership and residence in the subject property. All signatures on final loan documents are notarized.
 - b. Applicants for Small Business Loans administered by the Office of Economic Development. No new loans are being offered under this program. Borrowers were required to provide personal identification including Social Security Number and Driver's License Number. If real property was provided as security for the loan, then deeds of trust and deeds of re-conveyance loan documents were notarized.
 - c. Applicants for Future Teacher Loans administered by the Parks, Recreation and Neighborhood Services Department. No new loans are being offered under this program. Borrowers were required to provide personal identification including Social Security Number and Driver's License Number and tax return information. Notarization of loan documents was not required.

Access to Covered Account Information

- (1) Access to covered accounts is limited to authorized City personnel.
- (2) Any unauthorized access to or other breach of covered accounts is to be reported immediately to the Director of the Stakeholder Department or the Director's designee.

Credit Card Payments --- Applicable to Covered Accounts for Utility Services Only

Credit card payments made over the internet or through the call center using the City of San Jose's online services are processed through the City's third party vendor, Kubra. Kubra is Payment Card Industry Data Security Standard Certified (PCI DSS). The PCI DSS is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other

critical protective measures. This comprehensive standard is intended to help organizations proactively protect customer account data.

Receipts for utility accounts include only the last four digits of the credit or debit card or the bank account used for payment of the utility account.

Outside Service Providers

As mentioned above, the City's third party vendor, Kubra, processes online one time credit card payments for utility services. In addition, Kubra provides electronic payment processing for recurring debit/credit and checking account payments in accordance with Payment Card Industry Data Security Standards. Staff will report on Kubra's policies and procedures designed to detect, prevent and mitigate the risk of identity theft in its next report to the City Manager's Office.

The City also utilizes as third party vendor, AmeriNational Community Services Inc., to service Housing Rehabilitation and Homebuyer loans. The City's contract with AmeriNational stipulates that the vendor must maintain confidentiality of client information, and that such information may be disclosed by the vendor only upon written authorization of the City, or as required by law. Staff will report on AmeriNational's policies and procedures designed to detect, prevent and mitigate the risk of identity theft in its next report to the City Manager's Office.

In the event the City engages a new service provider to perform an activity in connection with one or more covered accounts, the procuring City Department in conjunction with the Purchasing Division of the Finance Department, will require that the contract with the service provider addresses the services provider's policies and procedures designed to detect, prevent and mitigate the risk of identity theft. The procuring City Department and the Purchasing Division of the Finance Department will keep the City Manager's Office informed regarding the specific identity theft prevention provisions incorporated in the service provider's contract.

Sources and Types of Red Flags Applicable to Utility Accounts¹

The types of red flags listed below have been identified as those that apply to covered utility accounts:

Suspicious documents:

- a. An application that appears to have been altered or forged, or appears to have been destroyed and reassembled.

¹ A full list of Red Flags listed in the Federal Trade Commission Regulations for creditors to consider in adopting their identity theft prevention programs can be found at Appendix A.

Suspicious personal identification, such as suspicious address change.

- b. The applicant or customer cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.

Unusual use of or suspicious activity relating to a covered account.

- 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 of unauthorized charges or transactions in connection with a customer's account.
- e. The 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.

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

Sources and Types of Red Flags Applicable to Loan Accounts

The types of red flags listed below have been identified as those that apply to the Office of Economic Development's maintenance of the existing Revolving Loan Fund Program accounts:

- a. An account is used in a manner that is not consistent with established patterns of activity on the account. For example:
 - i. Nonpayment when there is no history of late or missed payments.
- b. Mail sent to the customer is returned repeatedly as undeliverable transactions continue to be conducted in connection with the customer's account.

The types of red flags listed below have been identified as those that apply to the Parks Recreation and Neighborhood Services Department's maintenance of the existing Future Teacher Loan Fund Program accounts:

Alerts from a consumer reporting agencies, fraud detection agencies or service providers.

- a. A fraud or active duty alert that is included with a consumer report.
- b. A notice of credit freeze in response to a request for a consumer report.
- c. A notice of address discrepancy provided by a consumer reporting agency.

Suspicious documents:

- d. An applicant's college transcripts appears to have been altered or forged.
- e. Inconsistency between the applicant's stated address and the address on supporting documents.

- f. 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.

Suspicious personal identification, such as suspicious address change.

- g. Personal identifying information provided by the customer is not consistent with other personal identifying information provided by the customer, such as a lack of correlation between the SSN range and date of birth.
- h. 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;
- i. The applicant or customer cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.

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

Unusual use of or suspicious activity relating to a covered account.

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

The types of red flags listed below have been identified as those that apply to the following loan programs offered by the Housing Department: Housing Rehabilitation, Teacher Homebuyer, San Jose State University Faculty and Staff Homebuyer, and Equity-Share Homebuyer:

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

- a. A fraud or active duty alert that is included with a consumer report;
- b. A notice of credit freeze in response to a request for a consumer report;
- c. A notice of address discrepancy provided by a consumer reporting agency;
- d. 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:
 - i. A recent and significant increase in the volume of inquiries;
 - ii. An unusual number of recently established credit relationships;
 - iii. A material change in the use of credit, especially with respect to recently established credit relationships; or
 - iv. An account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor.

Suspicious documents. Examples of suspicious documents include:

- e. Documents provided for identification that appear to be altered or forged;
- f. Identification on which the photograph or physical description is inconsistent with the appearance of the applicant or customer;
- g. Identification on which the information is inconsistent with information provided by the applicant or customer;
- h. An application that appears to have been altered or forged, or appears to have been destroyed and reassembled.

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:
 - i. The address does not match any address in the consumer report; or
 - ii. The Social Security Number (SSN) has not been issued, or is listed on the Social Security Administration's Death Master File.
- j. Personal identifying information provided by the applicant is not consistent with other income or residence documents provided by the applicant.
- k. Personal identifying information provided by the applicant is not consistent with other income or residence documents provided by the applicant.
- l. Personal identifying information 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.
- m. 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.
- n. Personal identifying information is not consistent with personal identifying information that is on file with the financial institution or creditor.

Prevention and Mitigation of Identity Theft

Existing Accounts

- (1) 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 will use his/her discretion to determine whether such red flag or combination of red flags suggests a threat of identity theft. If such employee determines that identity theft or attempted identity theft is likely or probable, such employee will report such red flags to his/her immediate supervisor. If such employee deems that identity theft is unlikely or that reliable information is available to reconcile red flags, the employee will convey this information to his/her supervisor who may in his/her discretion determine that no further action is necessary. If it is determined that further

City of San Jose
ITPP, October 15, 2008

action is necessary, a City employee will perform one or more of the following responses, as determined to be appropriate by his/her supervisor:

- a. Notify the customer regarding the information that indicates the threat of identity theft;
- b. Close the account.
- c. If applicable, cease attempts to collect additional charges from the customer and decline to sell or transfer 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;
- d. If applicable, notify a debt collector of the discovery of likely or probable identity theft relating to a customer account that has been sold to or is being serviced by such debt collector in the event that a customer's account has been transferred to a debt collector prior to the discovery of the likelihood or probability of identity theft relating to such account;
- e. In the event that someone other than the customer has accessed the customer's covered account causing additional charges to accrue or accessing personal identifying information, notify the Department Director or the Director's designee. The Department Director or the Director's designee will then determine whether further notifications to the City Manager's Office, City Attorney's Office and/ or the San Jose Police Department are warranted under the circumstances; or
- f. Take other appropriate action to prevent or mitigate identity theft.

New Accounts

(2) 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 to an application for a new account, such employee will use his/her discretion to determine whether such red flag or combination of red flags suggests a threat of identity theft. If such employee determines that identity theft or attempted identity theft is likely or probable, such employee will report such red flags to his/her immediate supervisor. If such employee deems that identity theft is unlikely or that reliable information is available to reconcile red flags, the employee will convey this information and determine that no further action is necessary. If further action is necessary, a City employee will perform one or more of the following responses, as determined to be appropriate by his/her manager:

- a. Request additional identifying information from the applicant;
- b. Deny the application for the new account;

- c. Notify the Stakeholder Department Director or the Director's designee, who will then determine whether further notifications to the City Manager's Office, City Attorney's Office and/or the San Jose Police Department are warranted under the circumstances; or
- d. Take other appropriate action to prevent or mitigate identity theft.

Updating the Program (Program Administration)

The City Manager's Office ("CMO") will annually review and update the Identity Theft Prevention Program along with any relevant red flags in order to reflect changes in risks to customers or to the safety and soundness of the City and its covered accounts from identity theft. In so doing, the CMO will consider the following factors and exercise its discretion in amending the program:

- (1) The City's experiences with identity theft;
- (2) Updates in methods of identity theft;
- (3) Updates in customary methods used to detect, prevent, and mitigate identity theft;
- (4) Updates in the types of accounts that the City offers or maintains; and
- (5) Updates in service provider arrangements.

Program Administration

Senior Staff within the Stakeholder Departments ("Senior Staff") are responsible for oversight of the Program and for Program implementation and will be responsible for preparing reports to the City Manager's Office related to compliance with the Program and recommendations for changes to the Program ("Program Reports"). The City Manager's Office will review Program Reports and will oversee the implementation of material changes to the Program, as necessary in the opinion of the City Manager, to address changing identity theft risks and to identify new or discontinued types of covered accounts. Any recommended material changes to the program, as determined by the City Manager, will be submitted to the City Council for consideration

- (1) Senior Staff will report to the City Manager at least annually, on compliance with the red flag requirements. The report will address material matters related to the Program and evaluate issues such as:
 - a. 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;
 - b. Service provider arrangements;
 - c. Significant incidents involving identity theft and management's response; and

d. Recommendations for material changes to the Program.

- (2) Senior Staff within each Stakeholder Department are responsible for providing training to all employees within the Stakeholder Department who are 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 the Identity Theft Prevention Program. The Senior Level Staff will exercise his or her discretion in determining the amount and substance of training necessary.

PROCEDURES RELATED TO NOTICES OF ADDRESS DISCREPANCIES

Notification of Address Discrepancy

Each City department who uses consumer reports in the performance of the department's function will assign a supervisory level staff person (Consumer Report Supervisor) with oversight of the use of consumer reports within the department. In the event that a City department that requested a consumer report receives a notice of address discrepancy from a consumer reporting agency, the City department will assign a staffperson under the supervision of the Consumer Report Supervisor to perform the following:

- (1) Compare the information in the consumer report with:
 - a. If applicable, information the City obtains and uses to verify a consumer's identity in accordance with the requirements of the Customer Information Program rules implementing 31 U.S.C. § 5318(l);
 - b. Information the City department maintains in its own records, such as applications for service, change of address notices, other customer account records;
 - c. Information the City obtains from third-party sources that are deemed reliable by the relevant City employee; or

- (2) Verify the information in the consumer report with the consumer.

Furnishing Consumer's Address to Consumer Reporting Agency

- (1) In the event that the City department reasonably confirms that an address provided by a consumer to the City department is accurate, the City department is required to provide such address to the consumer reporting agency from which the City department received a notice of address discrepancy with respect to such consumer. This information is required to be provided to the consumer reporting agency when:
 - a. The Consumer Report Supervisor is able to form a reasonable belief that the consumer report relates to the consumer about whom the City requested the report;
 - b. The City establishes a continuing relationship with the consumer; and
 - c. The City regularly and in the ordinary course of business provides information to the consumer reporting agency from which it received the notice of address discrepancy.

**City of San Jose
ITPP, October 15, 2008**

- (2) Such information will be provided to the consumer reporting agency as part of the information regularly provided by the City to such agency for the reporting period in which the City establishes a relationship with the consumer.

Methods of Confirming Consumer Addresses

The City staff person under the director of a Consumer Report Supervisor may, in his or her discretion, confirm the accuracy of an address through one or more of the following methods:

- (1) Verifying the address with the consumer;
- (2) Reviewing the City's records to verify the consumer's address;
- (3) Verifying the address through third party sources; or
- (4) Using other reasonable processes.

Appendix A

Sources and Types of Red Flags

The red flags listed below are set forth in the FTC Regulations for creditors to consider in adopting their identity theft prevention programs. The types of red flags listed below do not apply to all covered accounts. The City has identified the red flags applicable to the utility covered accounts and the loan covered accounts as stated in the City's Identity Theft Prevention Program.

- (1) Alerts from consumer reporting agencies, fraud detection agencies or service providers. Examples of alerts include but are not limited to:
 - a. A fraud or active duty alert that is included with a consumer report;
 - b. A notice of credit freeze in response to a request for a consumer report;
 - c. A notice of address discrepancy provided by a consumer reporting agency;
 - d. 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:
 - i. A recent and significant increase in the volume of inquiries;
 - ii. An unusual number of recently established credit relationships;
 - iii. A material change in the use of credit, especially with respect to recently established credit relationships; or
 - iv. An account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor.
- (2) Suspicious documents. Examples of suspicious documents include:
 - a. Documents provided for identification that appear to be altered or forged;
 - b. Identification on which the photograph or physical description is inconsistent with the appearance of the applicant or customer;
 - c. Identification on which the information is inconsistent with information provided by the applicant or customer;
 - d. 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
 - e. An application that appears to have been altered or forged, or appears to have been destroyed and reassembled.

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

- a. Personal identifying information that is inconsistent with external information sources used by the financial institution or creditor. For example:
 - i. The address does not match any address in the consumer report; or
 - ii. The Social Security Number (SSN) has not been issued, or is listed on the Social Security Administration's Death Master File.
- b. Personal identifying information provided by the customer is not consistent with other personal identifying information provided by the customer, such as a lack of correlation between the SSN range and date of birth;
- c. 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;
- d. 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;
- e. The SSN provided is the same as that submitted by other applicants or customers for the same type of covered account;
- f. 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 for the same type of covered account;
- g. 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;
- h. Personal identifying information is not consistent with personal identifying information that is on file with the financial institution or creditor; or
- i. The applicant or customer cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.

(4) Unusual use of or suspicious activity relating to a covered account. Examples of suspicious activity include:

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

City of San Jose
ITPP, October 15, 2008

- i. The customer fails to make the first payment or makes an initial payment but no subsequent payments.
 - c. An account is used in a manner that is not consistent with established patterns of activity on the account. There is, for example:
 - i. Nonpayment when there is no history of late or missed payments;
 - ii. A material change in purchasing or spending patterns;
 - d. An account that has been inactive for a long period of time is used (*taking into consideration the type of account, the expected pattern of usage and other relevant factors*).
 - e. Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's account.
 - f. The City is notified that the customer is not receiving paper account statements.
 - g. The City is notified of unauthorized charges or transactions in connection with a customer's account.
 - h. The 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.
- (5) Notice from customers, law enforcement, victims or other reliable sources regarding possible identity theft or phishing relating to covered accounts.