



City of Woodland

REPORT TO MAYOR AND CITY COUNCIL

AGENDA ITEM

TO: THE HONORABLE MAYOR
AND CITY COUNCIL

DATE: October 20, 2009

SUBJECT: Policy – Identity Theft Prevention “Red Flag”

Report in Brief

In 2003, Congress enacted the Fair and Accurate Credit Transactions Act (FACTA) to curtail the effects of identity theft. The Act has been amended to now include local government agencies as creditors as these agencies defer payments for goods or services, such as payments for utilities or payment plans for parking tickets. The City is required to establish policies and procedures to help prevent identity theft relating to the tenets of the Act.

Staff recommends that the City Council approve Resolution No. _____ to adopt an Identity Theft Prevention Policy for the City of Woodland as described herein.

Background

The City Attorney’s office has been advising and providing the City with information and sample policies for several months on the implementation of FACTA, as well as, advice on how it will affect City operations. In November, 2007, the Act added provisions to the Federal Credit Reporting Act called the “Red Flag Rules” to help prevent identity theft. This provision of the Act became effective on January 1, 2008. There have been several iterations of the final Rules which were originally to be implemented not later than May 1, 2008. Continual updates necessitated postponements to November 1, 2008, May 1, 2009, August 1, 2009 and finally November 1, 2009. At this point it is believed the November 1, 2009 date will be the final extension. The City’s proposed Policy and Procedures are ready for Council consideration and adoption at this time.

Discussion

The Act was designed to create triggers or “red flags” to alert that a consumer with a covered account may be a victim of identity theft. While the City has little ongoing credit with individuals, there may be instances where there could be covered accounts that would provide for such ongoing payments. One such instance could be where a consumer has failed to pay utilities for an extensive period of time and works with the City to set a payment schedule to bring the account current. The

consumer could be utilizing their credit card to affect these payments. This sample instance could create a vehicle for identity theft.

Staff will become aware of identification methods outlined in the proposed Policy on how to detect and report possible identity theft of covered accounts. These efforts will assist Woodland citizens in early detection and reporting of possible misuse of their accounts, credit cards, etc.

Annual reports are required to insure adherence to the Policy and determine whether updates or revisions are needed. The Director of Administrative Services or designee is the primary responsible party for implementation and direction under this policy and reporting. Staff from the City Attorney's Office and Finance has been involved in the development of the proposed Policy.

Fiscal Impact

The financial impact to the City should be minimal other than staff time to implement, monitor and report occurrences. There are fines to be levied by "government regulators" should staff disregard red flags resulting in a loss to consumers.

Public Contact

Posting of the City Council agenda.

Recommendation for Action

Staff recommends that the City Council approve Resolution No. _____ to adopt an Identity Theft Prevention Policy for the City of Woodland as described herein.

Prepared by: Sue Vannucci, Director of
Administrative Services

Mark G. Deven
City Manager

Attachments: Resolution
Proposed Policy

CITY OF WOODLAND

IDENTIFY THEFT PREVENTION POLICY

New Identity Theft Prevention Policy

Purpose

The creation and implementation of an Identity Theft Prevention Policy for the City of Woodland that will identify, detect, mitigate, and update Red Flags that signal the possibility of identify theft in connection with the opening of a covered account or any existing covered account.

Effective date:

TABLE OF CONTENTS

Part 1	Definitions	3
Part 2	Incorporation of Existing Procedure.....	4
Part 3	Identification of Relevant Red Flags	5
Part 4	Detection, Prevention and Mitigation	8
Part 5	Policy Updates	10
Part 6	Third Party Service Providers	10
Part 7	Additional Legal Requirements (if necessary)	11
Part 8	Administration	14
Part 9	Policy Approval	15
Part 10	Rehabilitation Housing Loans	16
Part 11	Policy Approval	24

PART 1 DEFINITIONS

Introduction

The City of Woodland is a public entity not selling tangible goods. The City does not act in the normal capacity of a vendor, nor issue credit. The City does allow payments of monthly utility bills and other services via credit card which may apply under the tenets of this law. The City is committed to the protection of those citizens who opt to utilize this form of payment for services rendered by the City.

1. For purposes of this Policy, the term "Covered Account" means an account that the City of Woodland offers or maintains, primarily for personal, family or household purposes, that involves or is designed to permit multiply payments or transactions **and** any other account that the City offers or maintains for which there is a reasonably foreseeable risk to customers or the safety and soundness of the City from identity theft, including financial, operational, compliance, reputation, or litigation risks.
2. For purposes of this Policy, the term "Identity Theft" means a fraud committed or attempted using the identifying information of another person without authority.
3. For purposes of this Policy, the term "Red Flag" means a pattern, practice, or specific activity that includes the possible existence of identity theft. Art 3 provides a specific description of which Red Flags are acceptable to this Policy.
4. For purposes of this Policy, the term "FACTA" means the Fair and Accurate Credit Transaction Act of 2003.
5. For purposes of this Policy, the term "Director of Administrative Services" means the Director of Administrative Services of the City of Woodland.
6. For purposes of this Policy, the term "Finance Officer" means the Finance Officer of the City of Woodland.

PART 2
INCORPORATION OF EXISTING POLICY AND PROCEDURE

The City of Woodland does not currently have any policy or procedure in place regarding identify theft.

PART 3
IDENTIFICATION OF RELEVANT RED FLAGS

After careful examination of our accounts, including the methods by which we open, access and past experience with identity theft, the following events/occurrences reasonably indicate the potential for identity theft and should be considered "Red Flags" for purposes of this Policy.

- A. Alerts, notifications, or other warnings received from consumer reporting agencies or service providers, such as fraud detection services. For the purposes of this Policy, the City of Woodland will seek to identify the "Red Flags" listed below:
1. A fraud or active duty alert is included with a consumer report.
 2. A consumer reporting agency provides notice of credit freeze in response to a request for a consumer report.
 3. A consumer reporting agency provides a notice of address discrepancy.
 - 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; or
 - d. An account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor.
- B. The presentation of suspicious documents, such as:
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 financial institution or creditor, 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.

PART 3
IDENTIFICATION OF RELEVANT RED FLAGS

- C. The presentation of suspicious personal identifying information, such as a suspicious address change:
10. Personal identifying information provided is inconsistent when compared against external information sources used by the City of Woodland. For example, the address does not match any address in the consumer report.
 11. Personal identifying information provided by the customer is not consistent with other personal identifying information provided by the customer.
 12. Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the City of Woodland. For example:
 - a. The address on an application is the same as the address provided on a fraudulent application; or,
 - b. The phone 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 financial institution or creditor. For example:
 - a. The address on an application is fictitious, a mail drop, or a prison; or,
 - b. The phone number is invalid, or is associated with a pager or answering service.
 14. 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 accounts or other customers.
 15. 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.
 16. Personal identifying information provided is not consistent with personal identifying information that is on file with the City of Woodland.

D. The unusual use of, or other suspicious activity related to, a covered account:

17. A new account is used in a manner commonly associated with known patterns of fraud patterns. For example, the customer fails to make the first payment or makes an initial payment but not subsequent payments.
18. A covered account is used in a manner that is not consistent with established patterns of activity on the account. There is, for example:
 - a. Nonpayment when there is no history of late or missed payments;
 - b. A material change in electronic fund transfer patterns in connection with a deposit account.
19. A covered account that has been inactive for a reasonably lengthy period of time is used.
20. Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's covered account.
21. The City of Woodland is notified that the customer is not receiving paper account statements.

E. Notice form customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts held by the City of Woodland:

22. The City of Woodland 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.

PART 4
DETECTION, PREVENTION AND MITIGATION

A. Detection

In an effort to ensure proper detection of any Red Flags, all customers (consumers) must provide a least the following information/documentation before any new covered account will be opened:

1. Full name;
2. Date of birth (individual);
3. Address, (a residential or business street address for an individual; for an individual who does not have a residential or business street address, an Army Post Office (APO) or Fleet Post Office (FPO) box number, or the residential or business street address of next of kin or of another contact individual; or for a person other than the individual (such as a corporation, partnership, or trust), a principal place of business, local office, or other physical location.

For any account holder of a covered account for which the above information is not already on file at the City of Woodland, the customer will be contacted within a reasonable period of time after discovering the missing information to obtain the necessary information.

To assist with detection of Red Flags, the City of Woodland, will implement the appropriate computer programs tailored to the City of Woodland business needs to help authenticate customers, monitor transactions, and change of address requests. Tyler-Eden Technologies Software upon implementation, will be used and the City of Woodland continued use of this program or one similar but of the equivalent status is incorporated and made part of this Policy.

B. Preventing and Mitigating Identity Theft

In the event that a Red Flag is detected, the City of Woodland is committed to preventing the occurrence of identity theft and taking the appropriate steps to mitigate any harm caused thereby. In order to respond appropriately to the detection of a Red Flag, the City of Woodland shall consider any aggravating circumstance(s) that may heighten the risk of identity theft. After assessing the degree of risk posed, the City will respond to the Red Flag in an appropriate manner, which may include:

1. Monitoring a covered account for evidence of identity theft;
2. Contacting the customer;
3. Reopening a covered account with a new account number;
4. Not opening a new covered account;
5. Closing an existing covered account;
6. Notifying law enforcement; or
7. Determining that no response is warranted under the particular circumstances

For the protection of our customers, all service providers hired by the City of Woodland to perform any activity in connection with any covered account must also take appropriate steps to prevent identity theft. To this end, the City of Woodland will only contract with service providers that have implemented the follow a similar identity theft prevention policy.

PART 5 POLICY UPDATES

The City of Woodland is committed to maintaining an Identity Theft Prevention Policy that is current with the ever-changing crime of identity theft. To that end, the City will reassess this Policy on a periodic basis. In reassessing this Policy, the City will add/delred Red Flags in Part 3 as necessary, to reflect changes to risks to customers or to the safety and soundness of the City fro identity theft. The determination to make changes to this Policy will fall within the discretion of the responsible parties identified in Part 7 of this Policy, but after careful consideration of the following:

1. The City of Woodland's past experience(s) with identity theft;
2. Changes in methods of identity theft;
3. Changes in methods to detect, prevent, and mitigate identity theft;
4. Changes in the types of accounts that the City offers or maintains; and,
5. Changes in the business arrangements of the City, including alliances, joint ventures, and service provider arrangements.

The Director of Administrative Services will designate the City's staff involved with the implementation of the Policy to prepare reports regarding the City's compliance with FACTA and the Red Flag rules requiring the implementation of an Identity Theft Prevention Policy. The reports should address material matters related to the Policy, such as the following:

1. The effectiveness of the City's Policies and Procedures to address the risk of identity theft in connection with opening customer accounts, as well as, with existing accounts. This includes identifying any issues related to identifying, detecting and responding to Red Flags;
2. Third-party service provider arrangements;
3. Significant incidents of identity theft or Red Flag detection, and the City's response to those incidents;
4. Recommendations for materials changes to the Policy to ensure that customer accounts are adequately protected from the risk of identity theft.

The reports should be prepared at least annually for review by the Director of Administrative Services or designee.

PART 6
THIRD PARTY SERVICE PROVIDERS

A. Oversight of Third Party Service Providers Involved with Customer Accounts

If the City employs a third-party service provider to perform any activity in connection with a customer account, the Director of Administrative Services or designee is responsible for ensuring that the activity is conducted in compliance with reasonable policies and procedures to detect, prevent and mitigate the risk of identity theft. This may be achieved by requiring that a third-party service provider has policies and procedures to detect the Red Flags identified by the City and also requiring the third party service provider to review the City's Policy and agree to report any Red Flag to the Director of Administrative Services or designee.

B. Use of Third Party-Service Provider to Assist in the Implementation of the Policy Involved with Customer Accounts

The City may hire a third-party service provider in order to implement this Policy. The third-party service provider may provide services such as the implementation and administration of computer software programs that detect Red Flags. If a third-party service provider is used to assist in the detection of Red Flags, the third-party service provider is required to immediately notify the Director of Administrative Services or designee if any Red Flags are discovered.

The Director of Administrative Services or designee is responsible for overseeing any third-party service provider in an appropriate and effective manner. The Director of Administrative Services or designee's oversight shall include periodic meetings and/or receipt and review of periodic reports from the third-party service provider regarding what services are being provided, any Red Flags that have been detected, and any possible modifications to the services provided to increase their effectiveness.

PART 7
ADDITIONAL REQUIREMENTS

A. Address Confirmation

The City shall furnish the consumer's address (if the address has been reasonably confirmed as accurate) to consumer reporting agencies as requested. In an effort to ensure that the City maintains accurate address information for its consumers and to ensure the City provides accurate address information of our consumers to reporting agencies, at least one of the following steps must be taken prior to providing the consumer's address to the consumer reporting agency:

- a) Verify the address on file with the consumer;
- b) Confirm the address being sent to the consumer reporting agency matches the address the City has on file for that particular consumer;
- c) Compare the address with information received from any third-party source; or
- d) Verify by other means that are reasonably available at that time.

B. Address Discrepancies

At least one of the following steps must be taken if the City receives notice from any consumer reporting agency that a substantial difference exists between the address for the consumer that the City provided and the address(es) in the consumer reporting agency's file for that particular consumer:

- a) Compare the differing address with the City's file by either (1) confirming that the address information provided by the City to the consumer reporting agency is the same information the City obtains and uses to verify the consumer's identity in accordance with the requirements of the Customer Information Program (CIP) rules (31 USC 5318(1) (31 CFR 103.121)); or (2) comparing the differing addresses with the City records and files, including any applications, change of address notifications, other customer account records, or retained CIP documentation; or (3) comparing the differing addresses with information the City may have received from a third-party sources; or,
- b) Verify the information in the consumer report provided by the consumer reporting agency, which can be done through any of the following methods:
 - Verify the information in the consumer report with the consumer.

- Verify the consumer's address through the records of applications, address change notifications and other account records for the consumer maintained by the City.
 - Verify the consumer's address through information from third parties.
 - Through the use of any other reasonable means.
- c) For newly established accounts for which a notice of address discrepancy was received, the City must provide the consumer reporting agency that furnished the notice of address discrepancy, the address that the City has reasonably confirmed to be accurate under the following circumstances:
- The City can form a reasonable belief that the consumer report relates to the consumer for whom the report was requested.
 - The City establishes a continuing relationship with the consumer; and,
 - The City regularly in the ordinary course of business provides the information to the consumer reporting agency from which the notice of address discrepancy was obtained
- d) The City must provide the consumer reporting agency the address that the City has reasonably confirmed to be accurate as part of the information the City regularly furnish for the reporting period in which the City establishes a relationship with the consumer.

PART 8
ADMINISTRATION

The City Council of the City of Woodland has designed the authority to develop, oversee, implement and administer the Policy to the Director of Administrative Services or designee. As part of the Director of Administrative Services or designee's oversight responsibilities for the Policy, the Director of Administrative Services or designee is required to review and approve all material changes to the Policy as necessary to address changing identity theft risks. The Director of Administrative Services or designee is also responsible for reviewing reports prepared by the City staff regarding compliance with FACTA and the Red Flag Rules requiring the implementation of an Identity Theft Prevention Policy.

The City staff that will be directly involved with opening customers' accounts or servicing customer accounts in a manner that would place them in a position to detect Red Flags, or allow them access to customer's private information shall be trained to detect Red Flags and appropriately respond when Red Flags are discovered. The City staff participation is crucial to the effective implementation of this Policy.

By signing below, I the Director of Administrative Services of the City of Woodland acknowledges that I or my designee will be responsible for overseeing the implementation, management, and updating of this new Policy and shall have the following responsibilities:

1. Assign specific responsibility for the Policy's implementation, including appropriate training for staff;
 - At least annually, the Director of Administrative Services will review the Policy's effectiveness, any service provider arrangements, significant incidents involving identity theft and City's response, and recommendations for ways to improve the Policy/
2. Review reports prepared by staff to ensure the City remains compliant with its legal responsibility to maintain an Identity Theft Prevention Policy, and,
3. Approve material changes to this Policy as necessary to address changing identity theft risks.

Susan L. Vannucci, Director
Administrative Services and Finance

Authorized Signature

Date

PART 10
REHABILITATION HOUSING LOANS

I. PURPOSE

The Fair and Accurate Credit Transaction Act of 2003 (FACTA), Section 114, as implemented by the Red Flag Rules, 16 C.F.R. § 681.2, issued by the Federal Trade Commission along with other federal agencies requires creditors of customer accounts to implement an Identity Theft Prevention Program. Pursuant to the regulations, the Redevelopment Agency of the City of Woodland and the City of Woodland (the "Agency" and the "City") are creditors because they provide Rehab Housing Loan services to customers prior to receipt of payment through customer accounts, which are maintained primarily for personal, family or household purposes and involve multiple payments or transactions, and for which there are a reasonable foreseeable risk of identity theft. Therefore the Agency and the City are required to implement an Identity Theft Prevention Program.

The purpose of this Identity Theft Prevention Program ("Program") is to detect, prevent and mitigate identity theft in connection with all customer accounts, taking into consideration the level of risk for identity theft given the Agency and City scope of services provided and the types of accounts. This Program is created to identify patterns, practices and specific activities that indicate the possible existence of identity theft, hereinafter referred to as "Red Flags". The Program sets forth the procedures for detecting Red Flags and responding to Red Flags when discovered.

II. DEFINITIONS

"Red Flag" shall mean a pattern, practice or specific activity that indicates the possible existence of identity theft as defined in the Red Flag Rules, and as specifically enumerated in Section V. 16 C.F.R. § 681.2.

"Identity Theft" shall mean a fraud committed or attempted using the personal identifying information of another person without his/her authority. 16 C.F.R. 603.2(a).

"Customer Account" shall mean a Rehab Housing Loan account or other account provided by the Agency and City that constitutes a "covered account" under the Red Flag Rules.

"Personal Identifying Information" shall mean information that may be used to identify a specific person, including, but not limited to, a social security number, date of birth, government issued driver's license or identification number, government passport

number, unique biometric data such as fingerprints or physical appearance, any unique electronic identification number, telephone number or address.

III. DESIGNATION OF AUTHORITY

The Agency Board and the City Council designate the authority to develop, oversee, implement and administer the Program to the City Director of Administrative Services or designee.

As part of the Director of Administrative Services' oversight responsibilities for the Program, the Director of Administrative Services is required to review and approve all material changes to the Program as necessary to address changing identify theft risks. The Director of Administrative Services is also responsible for reviewing reports prepared by the Agency and City staff regarding the Agency and City compliance with FACTA and the Red Flag Rules requiring the implementation of an Identity Theft Prevention Program.

IV. COMPLIANCE REPORTS TO BE PREPARED BY THE AGENCY AND CITY STAFF

The Director of Administrative Services will designate the Agency and City staff involved with the implementation of the Program to prepare reports regarding the Agency and City compliance with FACTA and the Red Flag Rules requiring the implementation of an Identity Theft Prevention Program. The reports should address material matters related to the Program, such as the following:

- (a) The effectiveness of the Agency and City Policies and Procedures to address the risk of identity theft in connection with opening customer accounts, as well as, with existing accounts. This includes identifying any issues related to identifying, detecting and responding to Red Flags.
- (b) Third party service provider arrangements;
- (c) Significant incidents of identity theft or Red Flag detection, and the Agency and City response to those incidents;
- (d) Recommendations for material changes to the program to ensure that customer accounts are adequately protected from the risk of identity theft.

The report should be prepared at least annually for review by the Director of Administrative Services or the Executive Director/City Manager and the Board and the Council.

V. RED FLAGS IDENTIFIED BY THE REDEVELOPMENT AGENCY

In identifying the Red Flags applicable to the Agency and City customer accounts, the Agency and City considered the following risk factors:

- (a) The types of accounts the Agency and City maintain and the types and categories of information maintained in each account file;
- (b) The methods the Agency and City provide to open customer accounts;
- (c) The methods the Agency and City provide to access customer accounts;
- (d) The Agency and City previous experience with identity theft on connection with the customer accounts.

The Red Flags identified in this Program have been incorporated from sources, which include supervisory guidance, past incidents of identity theft, and changes in methods of identity theft risk.

The Agency and City identified Red Flags are as follows:

Alerts, notifications or other warnings received from consumer reporting agencies or service providers providing fraud protection services:

- Fraud or active duty alerts from consumer reports.
- Notice of a credit freeze from a consumer reporting agency in response to request for a consumer report.
- Notice of address discrepancy provided by a consumer reporting agency.
- A consumer report indicates a pattern of activity that is inconsistent with the history or usual pattern of activity of a customer or applicant.
- Recent significant increase in the volume of inquiries of the customer's credit.
- Unusual number of recently established credit relationships.
- A material change in the use of credit, especially in regards to credit relationships recently established.
- A customer had an account with the Agency and City or any other creditor that was closed for cause or identified for abuse of account privileges.

Suspicious Documents:

- Documents used for identification purposes appear to have been altered or forged.
- The photograph or physical description on the identification documents do not match the appearance of the person presenting the documentation.
- Other information in identification documents does not match the information provided by the individual presenting the identification documentation.
- Other information in the identification documents does not match the information on file with the Agency and City.
- The application to open the account appears to have been forged, altered, or gives the appearance of having been destroyed and reassembled.

Suspicious Personal Identifying Information:

- Personal information provided is inconsistent with information provided by an external source, for example, where the address provided does not match the address contained in a consumer report.
- Personal identifying information is inconsistent with other personal identifying information provided by the customer, such as a date of birth and social security number that do not correlate.
- Personal identifying information provided is associated with known fraudulent activity, as indicated by internal or third-party sources, such as the address or phone number on an application was previously provided on another fraudulent application.
- The address or telephone number provided is the same as other individuals attempting to open an account or existing customers.
- The individual opening the account cannot provide all of the required personal identifying information for an application.
- Personal identifying information is inconsistent with the information provided by the customer on file with the Agency and City.

Unusual Use of or Other Suspicious Activity Related to a Customer Account:

- Mail sent to the customer is returned repeatedly.
- The Agency and City are notified that a customer is not receiving his/her paper account statements.
- The Agency and City are notified of unauthorized transactions on a customer's account.

Notice of Possible Identity Theft:

- The Agency and City are notified by a customer of possible identity theft in connection with his/her account.
- The Agency and City are notified by a victim of identity theft of possible identity theft in connection with a customer account.

- The Agency and City are notified by law enforcement of possible identity theft in connection with a customer account.
- The Agency and City are notified by others of possible identity theft in connection with a customer account.

VI. PROCEDURES FOR DETECTING RED FLAGS

The following procedures are being implemented by the Agency and City to detect the Red Flags identified with opening of accounts and existing accounts identified above:

- (a) Obtain personal identifying information of an individual to verify his/her identity prior to opening an account, which includes the following:
 - (1) Full Name.
 - (2) Date of Birth.
 - (3) Residential Street Address.
- (b) Authenticate the identity of customers when they are requesting information about their accounts.
- (c) Authenticate the identity of customers when they are requesting to make any changes to their accounts.
- (d) Verify the validity of all billing address change requests.
- (e) Conduct a credit check when opening anew account.
- (f) Monitor transactions.
- (g) Verify all requests to change banking information used for payment.

Members of the Agency and City staff will be assigned and trained to detect Red Flags.

In addition, the Agency and City may employ the services of a third party service provider and/or utilize computer software programs to assist in detecting Red Flags.

VII. PROCEDURES FOR RESPONDING TO RED FLAGS

In order to prevent and mitigate identity theft, and after taking into consideration the risks of identity theft applicable to the customer account, the Agency and City implement the following procedures to respond to all Red Flags that are discovered. One or more of these procedures will be used each time a Red Flag is detected:

- (a) Monitor accounts for evidence of identity theft.
- (b) Contact the customer.
- (c) Reopen an account with a new account number.
- (d) Close an existing account.
- (e) Not open a new account.
- (f) Notify law enforcement.
- (g) Determine that no response is warranted given the particular circumstances.
- (h) Ask the customer to appear in person with government issued identification.
- (i) Do not provide account information to anyone other than the account holder, or other individual authorized by the account holder.
- (j) Update all account information.
- (k) Initiate an investigation.

In addition to any of the actions above, the Finance Officer or designee, will be notified of any Red Flags discovered.

VIII. TRAINING OF STAFF

The Agency and City staff that will be directly involved with opening customers' account or servicing customer accounts in a manner that would place them in a position to detect Red Flags, or allow them access to customers' private information shall be trained to detect Red Flags and appropriately response when Red Flags are discovered. The Agency and City staff participation is crucial to the effective implementation of this Program.

The Director of Administrative Services or designee will oversee all staff training to ensure that training is adequate to ensure effective implementation of the Program.

IX. OVERSIGHT OF THIRD-PARTY SERVICE PROVIDER INVOLVED WITH CUSTOMER ACCOUNTS

If the Agency or City employs a third-party service provider to perform any activity in connection with a customer account, the Agency and City will ensure that the activity is conducted in compliance with reasonable policies and procedures to detect, prevent and mitigate the risk of identity theft. This may be achieved through various means, including but not limited to, requiring that a third-party service provider has policies and procedures to detect the Red Flags identified by the Agency and City and/or requiring the third-party service provider to review the Agency and City Program and agree to report any Red Flags to the Director of Administrative Services or designee.

X. USE OF A THIRD-PARTY SERVICE PROVIDER TO ASSIST IN THE IMPLEMENTATION OF THE PROGRAM

The Agency and City may hire a third-party service provider in order to implement this Program. The third-party service provider may provide services such as the implementation and administration of computer software programs that detect Red Flags. If a third-party service provider is used to assist in the detection of Red Flags, the third-party service provider is required to immediately notify the Director of Administrative Services or designee if any Red Flags are discovered.

The Director of Administrative Services or designee is responsible for overseeing any third-party service provider in an appropriate and effective manner. The Director of Administrative Services oversight shall include periodic meetings and/or receipt and review of periodic reports from the third-party service provider regarding what services are being provided any Red Flags that have been detected, and any possible modifications to the services provided to increase the effectiveness

XI. PERIODIC IDENTIFICATION OF CUSTOMER ACCOUNTS

The Director of Administrative Services shall periodically review the types of accounts it maintains for customers to determine which are "covered accounts" under the Red Flag Rules and therefore are subject to this Program.

XII. PERIODIC UPDATE OF THE PROGRAM

This Program shall be updated periodically to ensure that the identified Red Flags, the procedures to detect Red Flags, and the responses to the Red Flags when discovered adequately protect customers from identity theft. The updating of the a Program should take into consideration any changes in the customers' level of risk of identity theft by looking at the following factors:

- (a) The Agency and City recent experiences with identity theft in connection with the customer accounts.
- (b) Changes in methods of identity theft.
- (c) Changes in methods of detecting, preventing, and mitigating identity theft.
- (d) Changes in types of customer accounts offered.
- (e) Changes in arrangements with any third-party service providers involved in the implementation of the Program.

The Agency and City staff or the Director of Administrative Services may recommend modifications to the program. However, any modification to the Program may not be implemented unless first approved by the Executive Director/City Manager or the Agency Board and City Council.

PART 11
POLICY APPROVAL

This Identity Theft Prevention Policy is hereby made a Policy of the City of Woodland effective on November 1, 2009 as authorized by the City Council.

Dated: October 2-, 2009

Mark G. Deven, City Manager

Susan L. Vannucci, Director, Administrative
Services and Finance