CITY OF
HAYWARD
HEART OF THE BAY

4

DATE: April 7, 2009

TO: Mayor and City Council
Redevelopment Agency

FROM: Director of Finance
Director of Public Works

SUBJECT: Adopting an Identity Theft Prevention Program and Policy in order to comply with 16 CFR § 681.2 (Fair & Accurate Credit Transaction Act of 2003).

RECOMMENDATION

That Council and Redevelopment Agency adopt the attached resolutions authorizing the implementation of an Identity Theft Prevention Program and Policy for the City of Hayward.

BACKGROUND

The acceptance and implementation of the program and policy will ensure compliance under the Fair and Accurate Credit Transactions (FACT) Act. The FACT Act of 2003 included a number of amendments to the Fair Credit Reporting Act (FCRA) aimed at protecting the privacy of the information in a consumer's credit report, assisting victims of identity theft, and preventing fraudulent credit transactions.

Congress enacted the Fair & Accurate Credit Transactions ("FACT") Act of 2003 to curtail the affects of identity theft. Recently the Act was amended to require all creditors, including local governmental agencies that defer payments for goods or services (such as utility payments and loan programs) to implement an identity theft prevention program utilizing warning signs, so called "red flags", as indicators of identity theft, e.g., altered identification documents or inconsistent personal identifying information.

In accordance with the FACT Act, creditors must determine whether covered accounts are subject to a risk of identity theft and, if necessary, implement a consumer credit protection program designed to detect, prevent, and mitigate identity theft in customer accounts. The program also should incorporate the creditor's existing policies and procedures where applicable, and provide for continued administration of consumer credit protections. The Act requires that such a program be approved and implemented by May 1, 2009.

To meet the mandates of the FACT Act, City staff performed a needs assessment taking into account the existing business practices, policies, and procedures currently in place to safeguard customer identity, account information, and financial transactions associated with customers' utilities and other accounts. Some policies and procedures, when appropriate, were modified to incorporate the basic elements for detecting, preventing, and mitigating identity theft.

DISCUSSION

The *Identity Theft Prevention Program* and *Identity Theft Prevention Policy* are policies and procedures to assist staff in the protection of the customers of the City of Hayward from unauthorized use or attempted use of any identifying information of a customer

The program includes procedures and other policies to (a) identify any "red flags" relevant to its customer accounts; (b) detect "red flags" relevant to customer accounts; (c) appropriately respond to any detected "red flags" to prevent and mitigate identity theft; and (d) ensure periodic updating of the program to reflect changes in risks to its customers and the City.

The proposed *Identity Theft Prevention Program* and *Identity Theft Prevention Policy* (ITPPs) attached for Council's approval takes into account the results of the needs assessment and analysis of the "red flag rules" issued by the Federal Trade Commission. The ITPPs will provide guidelines for the City to notify affected individuals in the case of actual identity theft, notify local law enforcement if appropriate, and provide secure handling of both electronic and paper documentation containing personally identifiable information.

The Program requires annual review and reporting to the City Manager. The Program also outlines improvements to our document storage systems.

FISCAL AND ECONOMIC IMPACT

There are fiscal impacts related to this recommendation, such as time necessary for staff training, additional locking cabinets, and possible costs and staff time to monitor third party service providers.

SCHEDULE

To meet the required implementation date of May 1, 2009, staff will need to be trained in the appropriate procedures for handling and storing sensitive customer data.

Prepared by:

Alex Ameri, Deputy Director of Public Works
Utilities

Recommended by:

Debra C. Auker, Director of Finance

Robert A. Bauman, Director of Public Works

Approved by:

Gregory T. Jones, City Manager

Attachments: A- City of Hayward Identity Theft Prevention Program
B - City of Hayward Identity Theft Prevention Policy
Draft Resolution

Identity Theft Prevention Program

CITY OF
HAYWARD
HEART OF THE BAY

Identity Theft Prevention Program

For

City of Hayward

777 B Street

Hayward, CA 94541

May 1, 2009

City of Hayward Identity Theft Prevention Program

This Program is intended to identify red flags that will alert our employees when new or existing accounts are opened using false information, protect against the establishment of false accounts, methods to ensure existing accounts were not opened using false information, and measures to respond to such events.

PREPARED IN ACCORDANCE WITH THE

FAIR AND ACCURATE CREDIT TRANSACTION ACT OF 2003

Purpose.

The purpose of this Program 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 for customers of the City of Hayward.

All utilities/municipalities are required to comply with this regulation. The Red Flag Rule requires any entity where there is a risk of identity theft, to develop and implement an Identity Theft Prevention Program. The Program must include reasonable policies and procedures for detecting, preventing, and mitigating identity theft. The rule was issued by the Federal Reserve System, the Federal Deposit Insurance Corporation, the Federal Trade Commission, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision. The compliance date is May 1, 2009 and includes all U.S. utilities/municipalities.

Definitions.

For purposes of this Program, the following definitions apply:

(a) "City" means the City of Hayward and Hayward Redevelopment Agency.
(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) "Person" means a natural person, a corporation, government or governmental subdivision or agency, trust, estate, partnership, cooperative, or association.
(g) "Personal Identifying Information" means a person's name, credit card account information, debit card information, bank account information, drivers' license information, date of birth, federal employer identification number (FEIN), and for a natural person includes their social security number.

(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.

Findings.

(1) The City is a creditor pursuant to 16 CFR § 681.2 due to its provision or maintenance of accounts for which payment is made in arrears and as a Lender in loan programs.

(2) Accounts offered to customers for the provision of city services include water, wastewater, loan programs and other related charges/fees.

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

(4) City limits access to personal identifying information to those employees responsible for or otherwise involved in opening or restoring accounts or accepting payment for use of accounts.

Table of Contents

Section 1 – Identifying "Red Flags" 6

Section 2 -Response to Attempted/Suspected Fraudulent Use of Identity 7

Section 3 -Customer Personal Identification Information 8

Section 4 -Physical Security of Personal Identifying Information Is Protected 9

Section 5 -Security of Electronic Records 9

Section 6 -Security Practices of Contractors and Outside Service Providers 10

Section 7 -Disposal of Sensitive Information 11

Section 8 –Program Administration and Periodic Updates to the Program 11

Section 9 -Reporting 11

Section 10 – Employee Training 12

Standard Operating Procedures
Identity Theft Prevention

Section 1 – Identifying "Red Flags"

The following have been identified as identity theft "red flags" relevant to the City.

Suspicious Documents

- Documents, provided for identification, which appear to be altered or forged.
- The photograph or physical description on identification is not consistent with the appearance of the applicant or customer presenting the identification.
- Other information on identification is not consistent with information provided by the person opening a new covered account or customer presenting the identification.
- Other information on 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.
- An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

Suspicious Personal Identifying Information

- Personal identifying information provided is inconsistent when compared against external information sources used by the financial institution or creditor. For example:
  a. The address does not match any address in the consumer report; or
  b. The Social Security Number (SSN) has not been issued, or is listed on the Social Security Administration's Death Master File.
- Personal identifying information provided is associated with known 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 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.
- 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.

- The SSN provided is the same as that submitted by other persons opening an account or other customers.
- 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.
- 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.
- Personal identifying information provided is not consistent with personal identifying information that is on file with the financial institution or creditor.

Notice from Customers, Victims of Identity Theft, Law Enforcement Authorities, or Other Reliable Sources Regarding Possible Identity Theft in Connection With Covered Accounts Held by the Financial Institution or Creditor.

- The financial institution or creditor 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.

Section 2 -Response to Attempted/Suspected Fraudulent Use of Identity

Internal Notification

Any City employee who becomes aware of a suspected or actual fraudulent use of a customer or potential customers identity must notify their supervisor and the Director of Finance or his/her designee.

Any employee that may suspect fraud or detect a red flag will implement the following response as applicable.

- Request applicant to provide additional identifying documentation;
- Deny the application for the new account;
- Close the account; or
- Take other appropriate action to prevent or mitigate identity theft, which may include contacting Hayward Police Department.

External Notification

Affected Individual – The City will notify the affected individual(s), if possible, of any actual identity theft. The following information will be included in the notice:

General information about the incident;

- The type of identifying information involved;

- Contact information for further information and assistance.

Method of Contact:

- Written notice, certified mail.
- E-mail, if the e-mail address is in the City records.
- By telephone, provided the contact is made directly with the affected person and appropriately documented.

Local Law Enforcement

The Hayward Police Department will be notified of any attempted or actual identity theft.

Oversight of Third Party Service Providers

The City will, as part of its contracts with third party service providers, require that providers have policies, procedures and programs that comply with the "Red Flag" Rule.

Section 3 -Customer Personal Identification Information

Information Collected

Identifying information is defined as **any name or number that may be used, alone or in conjunction with any other information, to identify a specific person.**

The following identifying information may be collected by this City.

- Name
- Social Security Number
- Date of Birth
- Official State /government issued driver's license or identification number,
- Employer or taxpayer identification number

How Customer Personal Identifying Information Is Collected

Customer personal identifying information may be collected by:

- Presentation by customer at the office;
- Telephone;
- Internet (future use);
- Mail.

Any other methods of collection are not acceptable.

Section 4 -Physical Security of Personal Identifying Information Is Protected

All paper documents or files, as well as CDs, floppy disks, zip drives, tapes, and backups containing personally identifiable information will be stored in locked file cabinets.

Files containing personally identifiable information are kept in locked file cabinets except when an employee is working on the file.

At the end of the day, employees put files away, log off their computers, and lock their file cabinets and office doors at the end of the day.

Building Access

Visitors who must enter areas where sensitive files are kept must be escorted by an employee of the City.

No visitor will be given any entry codes or allowed unescorted access to the office.

Section 5 -Security of Electronic Records

General Network Security

Anti-virus and anti-spyware programs will be run on individual computers and on servers on the network daily.

When sensitive data is received or transmitted, secure connections will be used.

Password Management

Computer passwords will be required.

Passwords will not be shared or posted near workstations.

User names and passwords will be different.

When installing new software, vendor-supplied default passwords will be immediately changed to a more secure strong password.

Laptop Security

The use of laptops is restricted to those employees who need them to perform their jobs.

Assess whether sensitive information really needs to be stored on a laptop. If not, delete it with a "wiping" program that overwrites data on the laptop.

Laptops are to be stored in a secure place.

Employees are never to leave a laptop visible in a car, at a hotel luggage stand, or packed in checked luggage unless directed to by airport security.

If a laptop must be left in a vehicle, it should be locked in a trunk.

Firewalls

The computer network will have a firewall where the network connects to the Internet.

Additional firewalls will be used to protect the computers on the network which store sensitive information.

Wireless and Remote Access

Encryption will be used when allowing remote access to the computer network by employees or by service providers.

Detecting Breaches

Monitor incoming traffic for signs of a data breach. Keep an eye out for activity from new users, multiple log-in attempts from unknown users or computers, and higher-than average traffic at unusual times of the day.

Monitor outgoing traffic for signs of a data breach. Watch for unexpectedly large amounts of data being transmitted from the system to an unknown user. If large amounts of information are being transmitted from the network, investigate to make sure the transmission is authorized.

The breach response plan will be maintained and updated as necessary.

Section 6 -Security Practices of Contractors and Outside Service Providers

In the event that City engages a service provider to perform an activity in connection with one or more covered accounts the Director of Finance or his/her designee 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.

Section 7 -Disposal of Sensitive Information

Paper Records

Paper records will be shredded before being placed into the trash.

Paper shredders will be available in the office or a document shredding service will be utilized.

Computers and Portable Storage Devices

When disposing of old computers and portable storage devices, use a Department of Defense-compliant disc wiping utility program.

Any data storage media (tapes, CD or DVD) will be disposed of by shredding, punching holes in, or incineration.

Section 8 –Program Administration and Periodic Updates to the Program

The Director of Finance or his/her designee is responsible for over-site of this Program, Program implementation, and reporting to the City Manager on issues related to this Program.

The Director of Finance will coordinate and review the program at least annually, or after each and every attempt at identity theft, and propose changes to the Program, as necessary.

Any proposed changes to the Identity Theft Prevention Program will be reviewed by the City Manager and City Attorney before being presented to the City Council for approval.

Section 9 -Reporting

The Director of Finance will report to the City Manager in June 2009, and with conclusion of the annual audit thereafter, on compliance with the "Red Flag" Rule. The report will include any material matters and issues regarding this program, such as:

- Initial implementation of the program;
- Employee training;
- Effectiveness of policies and procedures in addressing risk in how accounts are opened and maintained;
- Service provider (third party) arrangements;
- Significant incidents involving identity theft and management response;
- Recommendations for changes.

Section 10 – Employee Training

The Director of Finance or his/her 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 Director of Finance in coordination with the City Manager shall exercise their discretion in determining the amount and substance of training necessary.

Employee training and implementation of other controls, as noted below, will strengthen this security program.

Check references, fingerprinting and/or background checks before hiring employees who will have access to sensitive data.

Access to customer's personal identify information is limited to employees with a "need to know."

Establish procedures for confirming that workers who separate from the City no longer have access to sensitive information. Terminate their passwords, and collect keys and identification cards as part of the check-out routine.

Employees notify their manager immediately if there is a potential security breach, such as a lost or stolen laptop.

Employees who violate security policy are subjected to discipline, up to and including dismissal.

For computer security tips, tutorials, and quizzes for everyone on your staff, visit www.OnGuardOnline.gov .

This plan has been reviewed and adopted by the City of Hayward City Council. Appropriate employees have been trained on the contents and procedures of this Identity Theft Prevention Program.

This plan has been reviewed and adopted by resolution:

City of Hayward Resolution #: _____

Date: _____

A report will be prepared annually and presented to the above named governing body to include matter related to the program, the effectiveness of the policies and procedures, the oversight and effectiveness of any third party billing and account establishment entities, a summary of any identify theft incidents and the response to the incident, and recommendations for substantial changes to the program, if any.

City of Hayward

Identity Theft Prevention Policy

Responsible for Administering this Policy

Director of Finance and City Staff

Purpose

Implement a security program that is in compliance with the Fair and Accurate Credit Transaction (FACT) Act of 2003. This security program is intended to identify red flags that will alert our employees when new or existing accounts are opened using false information, protect against the establishment of false accounts, methods to ensure existing accounts were not opened using false information, and measures to respond to such events.

Background

On January 1, 2008, the Federal Trade Commission issued rules and guidelines for regulating the fraudulent use or attempt to use private, identifying information. These rules require that the City of Hayward (City) and Hayward Redevelopment Agency (RDA) develop and implement an identity theft prevention program.

These rules will be enforced beginning May 1, 2009.

Scope

This policy requires the safe keeping of certain account information kept by the City concerning its customers which is or can be used as identifying information. "Identifying information" means information such as a name, or number, that may be used, alone or in conjunction with any other information, to identify a specific person.

In this policy "personal identifying information" includes, but is not limited to, the following:

a. Name, social security number, date of birth, official State or government issued driver's license or identification number, employer or taxpayer identification number;
b. Any credit card account information, debit card information, or bank account information.

Policy Statement

The City shall implement the Identity Theft Prevention Program which includes reasonable procedures for detecting, preventing, and mitigating its customers from undue risk of identity theft.

Identity Theft Prevention Program

Staff will develop, and the City Council will approve an Identity Theft Prevention Program, designed to detect, prevent, and mitigate identity theft in connection with accounts in which the City or the RDA are creditors.

The program will include procedures and other policies to:

1. Identify any "Red Flags" relevant to its customer accounts;
2. Detect "Red Flags" relevant to customer accounts;
3. Appropriately respond to any detected "Red Flags" to prevent and mitigate identity theft.
4. Ensure periodic updating of the program to reflect changes in risks to its customers and the City.

Program Administration

Upon approval of this policy by the City Council, the City will:

1. Appoint the Director of Finance to oversee the development, implementation, and administration of the City's Identity Theft Prevention Program;
2. Train staff, as necessary, to effectively implement the program; and,
3. Exercise appropriate and effective oversight of outside service providers and other third party arrangements.

Oversight of Program

The Director of Finance will exercise oversight of the Identity Theft Prevention Program by:

(1) Assigning specific responsibility for the Program's Implementation.
(2) Reviewing reports prepared by staff regarding compliance with this Program; and,
(3) Submitting for Council approval any material changes to the Program as necessary to address changing identity theft risks.

Reporting

The Director of Finance or his/her designee will report to the City Manager at least annually on compliance with the Identity Theft Prevention Program.

The report should address material matters related to the Program and evaluate issues such as:

- The effectiveness of the policies and procedures in addressing the risk of identity theft in connection with the opening of covered accounts and with respect to existing covered accounts;
- Service provider arrangements;
- Significant incidents involving identity theft and management's response; and,

- Recommendations for material changes to the Program.

Oversight of Outside Service Provider Arrangements

Whenever this City engages a service provider to perform an activity in connection with one or more covered accounts, the City shall take steps to ensure that the activity of the service provider is conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft. The service provider shall be required by contract to have policies and procedures to detect relevant Red Flags that may arise in the performance of the service provider's activities, and either report the Red Flags to the City or take appropriate steps to prevent or mitigate identity theft.

_____

Adoption Date:

_____

Effective Date:

DRAFT

HAYWARD CITY COUNCIL

RESOLUTION NO._____

Introduced by Council Member_____

mae
3/23/09

RESOLUTION APPROVING POLICES AND PROCEDURES FOR AN IDENTITY THEFT PREVENTION PROGRAM IN ACCORDANCE WITH THE FAIR AND ACCURATE CREDIT TRANSACTION ACT OF 2003

WHEREAS, the Fair and Accurate Credit Transaction ("FACT") Act of 2003, was enacted by Congress to curtail the effect of identity theft; and

WHEREAS, the FACT Act was recently amended to require all creditors (including local governmental agencies that defer payments for goods or services) to implement an identity theft prevention program by establishing policies and procedures utilizing warning signs, so called "red flags", as indicators of identity theft; and

WHEREAS, in accordance with the FACT Act, creditors must determine whether covered accounts are subject to a risk of identity theft, and, if necessary, implement a program designed to detect, prevent, and mitigate identity theft in customer accounts. The program also should incorporate the creditor's existing policies and procedures where applicable, and provide for continued administration of consumer credit protections. The Act requires that such a program be approved and implemented by May 1, 2009; and

WHEREAS, in order to meet the mandates of the FACT Act, City staff performed a needs assessment, taking into account the existing business practices, policies and procedures currently in place to safeguard customer identity, account information and financial transactions associated with customers' utilities accounts and loan programs and, when appropriate modified or enhanced these policies and procedures to incorporate the four basic elements for detecting, preventing, and mitigating identity theft by enabling the City to:

1. Identify specific forms or activities that are "red flags" signaling possible identity theft and incorporate those "red flags" into the program;

2. Detect "red flags" that have been incorporated into the identity theft prevention program;

3. Respond appropriately to any "red flags" that are detected to prevent and mitigate identity theft; and

4. Ensure the identity theft prevention program is updated periodically to reflect changes in risks from identity theft; and

WHEREAS, to ensure compliance with the FACT Act, federal government regulators will be required to evaluate public agencies and their adherence to their identity theft prevention programs and when necessary, impose fines where the disregard of "red flags" has resulted in losses to consumers; and

WHEREAS, staff recommends approval of the Identity Theft Prevention Policy Program in accordance with the Fair and Accurate Credit Transaction Act of 2003 attached hereto as Exhibit "A"; and

WHEREAS, as indicated in the proposed Policy, staff has been assigned to develop, implement, and administer the proposed program and will create, at least annually, a report on its compliance with the FACT Act.

NOW, THEREFORE, BE IT RESOLVED that the City Council of the City of Hayward hereby approves the Policy Program in accordance with the Fair and Accurate Credit Transactions Act of 2003 as shown on Exhibit "A" attached hereto.

IN COUNCIL, HAYWARD, CALIFORNIA _____, 2009

ADOPTED BY THE FOLLOWING VOTE:

AYES: COUNCIL MEMBERS:
MAYOR:

NOES: COUNCIL MEMBERS:

ABSTAIN: COUNCIL MEMBERS:

ABSENT COUNCIL MEMBERS:

ATTEST:_____
City Clerk of the City of Hayward

APPROVED AS TO FORM:

_____
City Attorney of the City of Hayward

DRAFT

REDEVELOPMENT AGENCY OF THE CITY OF HAYWARD CITY

RESOLUTION NO._____

Introduced by Agency Member _____

Mole
3/23/09

RESOLUTION APPROVING POLICES AND PROCEDURES FOR AN IDENTITY THEFT PREVENTION PROGRAM IN ACCORDANCE WITH THE FAIR AND ACCURATE CREDIT TRANSACTION ACT OF 2003

WHEREAS, the Fair and Accurate Credit Transaction ("FACT") Act of 2003, was enacted by Congress to curtail the effect of identity theft; and

WHEREAS, the FACT Act was recently amended to require all creditors (including local governmental agencies that defer payments for goods or services) to implement an identity theft prevention program by establishing policies and procedures utilizing warning signs, so called "red flags", as indicators of identity theft; and

WHEREAS, in accordance with the FACT Act, creditors must determine whether covered accounts are subject to a risk of identity theft, and, if necessary, implement a program designed to detect, prevent, and mitigate identity theft in customer accounts. The program also should incorporate the creditor's existing policies and procedures where applicable, and provide for continued administration of consumer credit protections. The Act requires that such a program be approved and implemented by May 1, 2009; and

WHEREAS, in order to meet the mandates of the FACT Act, City staff performed a needs assessment, taking into account the existing business practices, policies and procedures currently in place to safeguard customer identity, account information and financial transactions associated with customers' utilities accounts and loan programs and, when appropriate modified or enhanced these policies and procedures to incorporate the four basic elements for detecting, preventing, and mitigating identity theft by enabling the City to:

1. Identify specific forms or activities that are "red flags" signaling possible identity theft and incorporate those "red flags" into the program;

2. Detect "red flags" that have been incorporated into the identity theft prevention program;

3. Respond appropriately to any "red flags" that are detected to prevent and mitigate identity theft; and

4. Ensure the identity theft prevention program is updated periodically to reflect changes in risks from identity theft; and

WHEREAS, to ensure compliance with the FACT Act, federal government regulators will be required to evaluate public agencies and their adherence to their identity theft prevention programs and when necessary, impose fines where the disregard of "red flags" has resulted in losses to consumers; and

WHEREAS, staff recommends approval of the Identity Theft Prevention Policy Program in accordance with the Fair and Accurate Credit Transaction Act of 2003 attached hereto as Exhibit "A"; and

WHEREAS, as indicated in the proposed Policy, staff has been assigned to develop, implement, and administer the proposed program and will create, at least annually, a report on its compliance with the FACT Act.

NOW, THEREFORE, BE IT RESOLVED that the City Council of the City of Hayward hereby approves the Policy Program in accordance with the Fair and Accurate Credit Transactions Act of 2003 as shown on Exhibit "A" attached hereto.

HAYWARD, CALIFORNIA _____, 2009

ADOPTED BY THE FOLLOWING VOTE:

AYES: AGENCY MEMBERS:
CHAIR:

NOES: AGENCY MEMBERS:

ABSTAIN: AGENCY MEMBERS:

ABSENT AGENCY MEMBERS:

ATTEST:_____
Secretary of the Redevelopment Agency
of the City of Hayward

APPROVED AS TO FORM:

_____
General Counsel