State of California

MEMORANDUM

To: Board of Directors **Date:** May 21, 2009

From: Steve Spears, Acting Executive Director
CALIFORNIA HOUSING FINANCE AGENCY

Subject: APPROVAL OF CalHFA's IDENTITY THEFT 'RED FLAG' PROGRAM

Pursuant to Section 114 of the Fair and Accurate Credit Transactions Act of 2003, (Pub. L. 108-159) the Federal Trade Commission added section 681 to its regulations (16 C.F.R. § 681) implementing the "Red Flag Rule", thereby requiring all users of consumer reports "to develop and implement a written Identity Theft Prevention Program.

The Rule states that the Identity Theft Prevention Program must provide for the identification, detection, and response to patterns, practices, or specific activities – known as 'red flags' - that could indicate identity theft. The 'Red Flag Rule' provides the opportunity to design and implement a program that is appropriate to their size and complexity.

CalHFA's Information Security Officer worked with staff and managers to develop an Identity Theft Program that meets the needs of CalHFA and the requirements of this Rule. This Program identifies CalHFA's relevant red flags and describes how each red flag may be detected and mitigated. A Program description document as well as policy and procedures have been developed to reflect the Program scope and requirements.

Title 16 CFR Section 681 also contains an unusual requirement that the Board of Directors of covered financial institutions and creditors specifically approve the provisions of the program. Consequently, the Agency is requesting Board approval of this matter.

RECOMMENDATION OF RESOLUTION 9-10

Resolution 9-10 would approve CalHFA's Identity Theft Prevention Program and designate the Executive Director to provide oversight of this Program. There is no cost associated with this resolution.

RESOLUTION 09-10

APPROVAL OF CALIFORNIA HOUSING FINANCE AGENCY'S (Agency) IDENTITY THEFT PREVENTION PROGRAM

WHEREAS, the Agency has existing Information Security and Privacy Programs that provide safeguards for the protection of CalHFA borrower's information, including identity theft prevention, and

WHEREAS, the Agency has existing procedures that protect our borrower's information that include 'red flags' for identity theft and fraud detection for our borrowers, and

WHEREAS, pursuant to Section 114 of the Fair and Accurate Credit Transactions Act of 2003, (Pub. L. 108-159) the Federal Trade Commission added section 681 to its regulations (16 C.F.R. § 681) implementing the "Red Flag Rule", thereby requiring all users of consumer reports "to develop and implement an Identity Theft Prevention Program, and

WHEREAS, the Agency plans to incorporate the "Red Flag Rule" requirements for identity theft prevention into their Information Security and Privacy Programs, and

WHEREAS, Title 16 Code of Federal Regulations section 681 requires that the Board of Directors of affected financial institutions and creditors approve the provisions of the Red Flag Program;"

NOW, THEREFORE, BE IT RESOLVED by the Board of Directors of the Agency as follows:

1. The Board approves the Identity Theft Prevention Program developed to implement the "Red Flag Rules", and
2. The Board authorizes the Executive Director to provide all future oversight for this program.

I hereby certify that this is a true and correct copy of Resolution 09-10 adopted at a duly constituted meeting of the Board of Directors of the Agency held on May 21, 2009, at Burbank, California.

ATTEST: ______________________
Secretary

CalHFA Identity Theft Prevention Program

I. PROGRAM ADOPTION

Pursuant to Section 114 of the Fair and Accurate Credit Transactions Act of 2003, (Pub. L. 108-159) the Federal Trade Commission added section 681 to its regulations (16 C.F.R. § 681.2) implementing the "Red Flag Rule', thereby requiring all users of consumer reports to develop and implement an Identity Theft Prevention Program (Program). California Housing Finance Agency (CalHFA) staff developed a Program which was reviewed by the Information Security Governance Committee and approved by the CalHFA Board of Directors on May 21, 2009. After consideration of the size and complexity of the CalHFA's operations, and the nature and scope of its activities, the Board of Directors and the Information Security Governance Committee determined that this Program was appropriate for CalHFA and therefore this Program will be incorporated into the CalHFA Information Security Program on June 1, 2009.

II. PROGRAM PURPOSE AND DEFINITIONS

A. Requirements of the Rule

Under the Red Flag Rule, every financial institution and creditor is required to establish an "Identity Theft Prevention Program" tailored to the size, complexity and nature of its operation. CalHFA is 'an assignee of an original creditor who participates in the decision to extend, renew or continue credit', and therefore is a creditor under the provisions of this rule. However, as CalHFA currently has a security and privacy program and is not a direct lender but only an intermediary in the loan process with no contractual agreements with our borrowers; the impact of this rule on CalHFA functions is minimal.

The Rule requires that the Identity Theft Prevention program contain reasonable policies and procedures to:

1. *Identify* relevant Red Flags for new and existing covered accounts and incorporate those Red Flags into the Program;
2. *Detect* Red Flags that have been incorporated into the Program;
3. *Respond* appropriately to any Red Flags that are detected to prevent and mitigate Identity Theft; and
4. *Ensure* the Program is updated periodically, to reflect changes in risks to customers or to the safety and soundness of the creditor from Identity Theft.

B. Red Flags Rule definitions used in this Program

The Red Flag Rule defines "Identity Theft" as "fraud committed using the identifying information of another person" and a "Red Flag" as "a pattern, practice, or specific activity that indicates the possible existence of Identity Theft." Under the Rule, a "covered account" is:

1. Any account CalHFA offers or maintains primarily for personal, family or household purposes, that involves multiple payments or transactions; and
2. Any other account CalHFA offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of CalHFA from identity theft.

III. IDENTIFICATION OF RED FLAGS.

CalHFA has conducted an internal review to evaluate which CalHFA functions would be impacted by this Rule. It was determined that the following Divisions within CalHFA fulfill a covered function under the rule. Reviewing these functions, we were able to identity which red flags are appropriate to prevent identity theft in CalHFA.

CalHFA determined that three of its Divisions will be impacted by this rule: Division of Accounting: Loan Servicing, Division of Mortgage Insurance: Underwriting and Quality Assurance and Division of Homeownership

There are five general categories of Red Flags. The Federal Trade Commission has provided five general categories and a list of 26 suggested Red Flags in the appendix to the Code of Federal Regulations. The categories and red flags that are applicable to CalHFA include:

<u>Alerts, Notifications or Warnings from a Consumer Reporting Agency</u>

- A fraud or active duty alert is included with a consumer report.
- A consumer reporting agency provides a notice of credit freeze in response to a request for a consumer report.
- A consumer reporting agency provides a notice of address discrepancy, as defined in § 681.1(b) of this part.
- Notice or report from a credit agency of an address discrepancy.

<u>Suspicious Documents</u>

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

<u>Suspicious Personal Identifying Information</u>

- 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 by the customer is not consistent with other personal identifying information provided by the customer. For example, there is a lack of correlation between the SSN range and date of birth.
- 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.
- Personal identifying information provided is not consistent with personal identifying information that is on file with the financial institution or creditor.

Unusual Use of, or Suspicious Activity Related to, the Covered Account

- 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 increase in the use of available credit;
    c. A material change in purchasing or spending patterns;
    d. A material change in electronic fund transfer patterns in connection with a deposit account; or
    e. A material change in telephone call patterns in connection with a cellular phone account.
- A covered account that has been inactive for a reasonably lengthy period of time is used (taking into consideration the type of account, the expected pattern of usage and other relevant factors).
- Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's covered account.
- The financial institution or creditor is notified that the customer is not receiving paper account statements.

Notice from Customers, Victims of Identity Theft, Law Enforcement Authorities, or Other Persons 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.

IV. DETECTION OF RED FLAGS

CalHFA will utilize the preceding list of red flags where appropriate to detect potential identity theft. This list is not intended to be all-inclusive and other suspicious activity may be investigated as necessary. Many of our current red flags used for fraud detection may also be used as red flags for identity theft.

Managers of the impacted Divisions identified these Red Flags and will train appropriate staff to recognize and respond to these Red Flags as they are encountered in the ordinary course of Agency business:

V. RESPONDING TO IDENTITY THEFT RED FLAGS

Many safeguards for protecting personal information from identity theft have already been defined in the CalHFA Information Security Policy Manual. CalHFA will incorporate the additional requirements of this new Identity Theft Prevention program into its existing Information Security Program.

Appropriate responses to detected Red Flags may include:

Monitoring an account;
Further investigation of an account;
Contacting the Lender;
Contacting the customer if we service their loan;
Closing or not approving an existing loan
Determining that no response is warranted under the particular circumstances.

VI. PROGRAM UPDATES

The Chief Deputy Director and the Information Security Governance Committee shall serve as Program Administrators. The Program Administrators will receive periodic reviews and updates on this Program to reflect changes in risks to customers from identity theft. In doing so, the Program Administrators will consider CalHFA's experiences with identity theft situations, changes in identity theft methods, changes in identity theft detection and prevention methods, and changes in CalHFA's business arrangements with other entities. After considering these factors, the Program Administrators will determine whether changes to the Program, including the listing of Red Flags, are warranted. If warranted, the Program Administrators will request an update to the Program.

VII. PROGRAM ADMINISTRATION

A. Oversight

Responsibility for administering, approving any updates to this Program, and reviewing Program reports lies with the Program Administrators.

The Information Security Officer (ISO) is responsible for working with CalHFA Division Managers to develop, implement and update this Program. The ISO will ensure all staff have appropriate training regarding the prevention and detection of identity theft.

Division Managers are responsible for ensuring appropriate training of their CalHFA staff related to their specific job functions, for reviewing any staff reports regarding the detection of Red Flags, for determining which steps of prevention and response should be taken in particular circumstances, and for considering periodic changes to the Program.

B. Staff Training and Reports

CalHFA staff that are responsible for implementing the Program shall be trained in the detection of Red Flags and the responsive steps to be taken when a Red Flag is detected. The Information Security Officer should prepare a report at least annually for the Program Administrators, including an evaluation of the effectiveness of the Program with respect to loan accounts, service provider arrangements, significant incidents involving identity theft and responses, and recommendations for changes to the Program.

C. Service Provider Arrangements

In the event CalHFA engages a service provider to perform an activity in connection with one or more accounts, the Agency will take the following steps to ensure the service provider performs its activity in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of Identity Theft.

1. Require, by contract, that service providers have such policies and procedures in place; and
2. Require, by contract, that service providers review CalHFA's Program and report any Red Flags to the Program Administrator.

CalHFA	Section 3050: Identity Theft Prevention Program
Information Security Policy Manual	Date: January 1, 2009 Revision No. NEW

GENERAL POLICY

The purpose of this policy is to incorporate an Identity Theft Prevention Program as part of the Information Security Program. This policy identifies the minimal components that must be considered as part of this program.

This policy requires the protection of any information concerning its customers, kept by CalHFA, which is or can be used as identifying information. "Identifying information" means any 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 "identifying information" includes, but is not limited to, the following:
a. Name, social security number, date of birth, driver's license or identification number, employer or taxpayer identification number;
b. Unique electronic identification number, address, or routing code; or
c. Any card, account number; personal identification number or other identifier.

All CalHFA staff shall protect its customers from undue risk of identity theft through information maintained by this Agency. In addition to protecting our customer's personal information by implementing the safeguards identified throughout the Information Security Policy Manual to prevent identity theft, staff must consider IdentityTheft Red Flags* that may identify this person has been a victim of identity theft when reviewing consumer credit reports and loan applications.

*A red flag is a pattern, practice, or specific activity that indicates the possible existence of Identity Theft.

Persons Affected: All staff.

STANDARDS:
Staff will develop, and the Board will approve an identity theft program, designed to detect, prevent, and mitigate identity theft in connection with the opening or servicing of a loan account. All Divisions that are considered either as 'maintaining a covered account' as defined by the Federal Trade Commission's Red Flag Rule or are 'users of consumer credit reports will develop and implement procedures to:

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

Appropriate responses to detected Red Flags may include:
Monitoring an account;
Further investigation of an account;

Contacting the Lender;
Contacting the customer if we service their loan;
Closing or not approving an existing loan
Determining that no response is warranted under the particular circumstances

Oversight of Service Provider Arrangements

Whenever this Agency contracts with or engages a service provider to perform any activity in connection with one or more covered accounts, the Agency 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 to have policies and procedures to detect relevant Red Flags that may arise in the performance of the service provider's activities on behalf of the Agency and either report the Red Flags to the Agency's Manager, or to take appropriate steps to prevent or mitigate identity theft.

PERSONAL INFORMATION SECURITY PROCEDURES

ROLES AND RESPONSIBILITIES:

Employees and Information Users	1. Comply with all policies and procedures pertaining to this Program. 2. Consider identity theft red flags when reviewing loan applications or consumer credit reports.
Division Managers	1. Ensure appropriate training of their staff related to identity theft prevention and detection in their specific job functions 2. Review any staff reports regarding the detection of Red Flags 3. Determine which steps of prevention and response should be taken in particular circumstances 4. Consider periodic changes to the Program.
Information Security Officer	1. Work with CalHFA Division Managers to develop, implement and update this Program. 2. Ensure all staff have appropriate training regarding the prevention and detection of identity theft. 3. Prepare a report at least annually for the Program Administrators, including an evaluation of the effectiveness of the Program with respect to loan accounts, service provider arrangements, significa incidents involving identity theft and responses, an recommendations for changes to the Program.
Chief Deputy Director and Information Security Governance Committee	1. Administer and approve any updates tot his Program 2. Review and approve Program reports.

	3. Determine whether changes to the Program, including the listing of Red Flags, are warranted. If warranted, the Program Administrators will request an update to the Program.