



Red Flag Policy and Identity Theft Prevention Program

Purpose

The purpose of the Red Flag Policy is to establish an Identity Theft Prevention Program. The program is designed to detect, prevent, and mitigate theft in connection with the opening of a covered account and an existing covered account to provide for continued administration of the Program in Compliance with Part 681 of Title 16 of the Code of Federal Regulations implementing Sections 114 and 315 of the Fair and Accurate Credit Transaction Act (FACTA) of 2003.

Definitions

Covered Account means:

1. An account that a creditor offers or maintains, primarily for personal, family or a household purpose that involves or is designed to permit multiple payments or transactions. Covered accounts include utility accounts; and
2. Any other account that the creditor offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and security of the creditor from identity theft, including financial, operational, compliance, reputation, or litigation risks.

Credit means the right granted by a creditor to a debtor to defer payment of debt or to incur debts and defer its payments or to purchase property or services or defer payment therefor.

Creditor means the right granted by the creditor to the debtor to defer payment of debt or to incur debts and defer its payments or purchase property or services and defer payment therefor.

Identifying information is any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including: name, address, telephone number, Social Security number, date of birth, government issued driver's license and/or identification number, unique electronic identification number, computer's Internet Protocol (IP) address, and/ or routing code.

Identity theft means fraud committed or attempted using the identifying information of another person without authority.

Red flag means a pattern, practice or specific activity that indicated the possible existence of identity theft.

The Program

Equity Smart Home Loans, Inc. has established an Identity Theft Prevention Program to detect, prevent and mitigate identity theft. The program shall include reasonable policies and procedures to:

1. Identify relevant red flags for covered accounts it offers or maintains and incorporates those red flags into the program;
2. Detect red flags 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 and to the safety and soundness of the creditor from identity theft.

The program shall, as appropriate, incorporate existing policies and procedures that control reasonably foreseeable risks.

Identification of Relevant Red Flags

In order to identify relevant Red Flags, the locality considers the types of accounts that offers and maintains, the methods it provides to open its accounts, the methods it provides to access its accounts and its previous experience with Identity Theft. **Equity Smart Home Loans, Inc** identifies the following red flags, in each of the listed categories:

A. Notifications and Warnings from Credit Reporting Agencies:

- a. Report of fraud accompanying a credit report;
- b. Notice or report from a credit agency of a credit freeze on a customer or application;
- c. Notice or report from a credit agency of an active duty alert for an applicant and indications from credit report of activity that is inconsistent with a customer's usual pattern or activity;

B. Suspicious Documents:

- a. Identification document or card that appears to be forged, altered or inauthentic;
- b. Identification document or card on which a person's photograph or physical description is not consistent with the person presenting the document and/or any other document with information that is not consistent with existing customers information (such as if a person's signature on a check appears forged);
- c. An Application for service that appears to have been altered or forged;

C. Suspicious Personal Identifying Information:

- a. Identifying information presented that is inconsistent with other information the customer provides (example: inconsistent birth dates);
- b. Identifying information presented that is inconsistent with other sources such as, address not matching an address on a credit report;
- c. Identifying information presented that is the same as information shown on other applications that were found to be fraudulent;
- d. Identifying information that is consistent with fraudulent activity such as, an invalid phone number or fictitious billing address;

D. Suspicious Account Activity or Unusual Use of Account:

- a. Change of address for an account followed by a request to change the account holder's name;
- b. Payments stop on an otherwise consistently up-to-date account;
- c. Account used in a way that is not consistent with prior use such as, someone with "Extremely High Activity";
- d. Mail sent to the account holder is repeatedly returned as "Undeliverable";
- e. Notice to the locality that a customer is not receiving mail sent by the locality;
- f. Notice to the locality that an account has "Unauthorized activity";
- g. Breach in the company's computer system security and/or unauthorized access to or use of customer account information;

E. Alerts from others:

- a. Notice to **Equity Smart Home Loans, Inc.** from a customer, identity theft victim, law enforcement and/or person that has opened or is maintaining a fraudulent account for a person engaged in Identity Theft.

Detection of Red Flags

A. **New Accounts:** In order to detect any of the Red Flags identified above, Equity Smart Home Loans, Inc. personnel will take the following steps to obtain and verify the identity of the person opening the account:

1. Require certain identifying information such as name, date of birth, residential or business address principal place of business for an entity, driver's license or other identification;
2. Verify the customer's identity by doing an assessment of their "Driver's License" and/or "Identification Card";
3. Review documentation showing the existence of a business entity;
4. Independently contact the customer;

Response to Suspected Identity Theft:

In the event of any identified Red Flags, **Equity Smart Home Loans, Inc.** personnel shall take one or more of the following steps, depending on the degree of risk posed by the Red Flag:

1. Contact the customer;
2. Notify the Program Administrator;
3. Notify Law Enforcement;

In order to further prevent the likelihood of identity theft occurring, **Equity Smart Home Loans, Inc.** will take the following steps with respect to its internal operating procedures to protect the customer's information:

1. Ensure all websites and/or servers are protected through our security servers protocol and/or virus protection is up to date;
2. Notice to customer regarding breach in security;
3. Ensure all office computers are "Password Protected," and all computer screens lock after a certain period of time;
4. Ensure that all paper documents and computer files containing customer information is destroyed in a timely manner;
5. Keep offices clear of papers containing customer information;
6. Request last 4 digits of Social Security numbers (if necessary);

7. Require that all personnel keep the required customer information that is solemnly needed for Mortgage Loan purposes.

Updating the Program

The program shall be updated periodically to reflect changes in risks to customers or the safety and soundness of the organization from identity theft based on factors such as:

1. The experience of the organization with identity theft;
2. Changes in methods of identity theft;
3. Changes in methods to detect, prevent and alleviate identity theft;
4. Changes in the types of accounts that the organization, including mergers, acquisitions, alliances, joint ventures and service provider arrangements;

Administration of Program

1. **Equity Smart Home Loans, Inc** (The government body, an appropriate committee of the governing body or a designated employee at the level of senior management shall be responsible for the development, implementation, oversight and continued administration of the program);
2. The program shall train staff, as necessary to effectively implement the program;
3. The program shall exercise appropriate and effective oversight to service provider arrangements;

Oversight of The Program Shall Include:

1. Assignment of specific responsibility for implementation of the program to the **Equity Smart Home Loans, Inc** manager or administrator;
2. Review reports prepared by staff regarding compliance;
3. Approval of material changes to the program as necessary to address changing risks of identity theft;

Reports Shall Be Prepared as Follows:

1. Staff responsible for development, implementation, and administration of the Program shall report to **Equity Smart Home Loans, Inc.** (The governing body, an appropriate committee of the governing body or a designated employee at the level of senior management) at least annually on compliance by the organization with the program.
2. The report shall address material matters related to the program and evaluate issues

such as:

- a. The effectiveness of the policies and procedures addressing the risk of identity theft in connection with the opening of covered accounts and with respect to existing covered accounts;
- b. Service provider agreements;
- c. Significant incidents involving identity theft and management's response;
- d. Recommendations for material changes to the program;

Oversight of Service Provider Arrangements

In the event **Equity Smart Home Loans, Inc.** engages a service provider to perform an activity in connection with one or more accounts, it 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;
2. Require, by contract, that service providers review **Equity Smart Home Loans, Inc.**;
3. Program and report any Red Flags to the program administrator;

Duties Regarding Address Discrepancies

Equity Smart Home Loans, Inc. shall develop policies and procedures designed to enable the organization to form a reasonable belief that a credit report relates to the consumer for whom it was requested if the organization received a notice of address discrepancy from a nationwide consumer reporting agency indicating the address given by the consumer differs from the address contained in the consumer report.

Equity Smart Home Loans, Inc. may reasonably confirm that an address is accurate by any of the following means:

1. Verification of the address with the consumer;
2. Review of the borrowers' records;
3. Verification of the address through third-party sources and/or reasonable means;

If an accurate address is confirmed, **Equity Smart Home Loans, Inc.** shall furnish the consumer's address to the nationwide consumer reporting agency from which it received the notice of address discrepancy if:

1. The organization establishes a continuing relationship with the consumer;
2. The organization, regularly and in the ordinary course of business, furnishes information to the Consumer reporting agency.

This completes **Equity Smart Home Loans, Inc.**'s Red Flag Policy.

Electronic Signature Binding: This Agreement and related documents may be accepted in electronic form (e.g., by an electronic or digital signature or other means of demonstrating assent) and each Party's acceptance will be deemed binding between the parties. Each Party acknowledges and agrees it will not contest the validity or enforceability of this Agreement and related documents, including under any applicable statute of frauds, because they were accepted and/or signed in electronic form.

I have read and understand **Equity Smart Home Loans, Inc.**'s policy regarding its Red Flag Policy and Identity Theft Prevention Program.

Printed Name

Date

Signature

Title