AUSTIN HOUSING
FINANCE CORPORATION

RBA: Approve AHFC Identity Theft Program Guidelines **AGENDA ITEM NO: 3**
CITY OF AUSTIN **AGENDA DATE: 03/03/2011**
RECOMMENDATION FOR BOARD ACTION **PAGE: 1 OF 1**

SUBJECT: Approve a resolution authorizing the adoption and implementation of a Customer Privacy Assurance Program for the Austin Housing Finance Corporation.

AMOUNT & SOURCE OF FUNDING:

FISCAL NOTE: There is no unanticipated fiscal impact. A fiscal note is not required.

REQUESTING DEPARTMENT: Austin Housing Finance Corporation

FOR MORE INFORMATION CONTACT: Elizabeth A. Spencer, Treasurer, Austin Housing Finance Corporation, 974-3182.

PRIOR BOARD ACTION:

PRIOR COUNCIL ACTION:

By this action, the Board of Directors adopts a resolution authorizing the Austin Housing Finance Corporation (AHFC) to implement a formal Customer Privacy Assurance Program to ensure the protection of consumer data and prevent identity theft.

The purpose of this program is to protect confidential information supplied by applicants to AHFC programs. Adoption will bring the AHFC into compliance with the federal Fair and Accurate Credit Transaction Act (FACTA).

FACTA requires businesses and organizations utilizing personal consumer data to implement a written identity theft prevention program which will assist the organization in detecting warning signs or "red flags" of identity theft in day-to-day operation, take steps to prevent such crimes, and control the resulting damage.

Approval of this resolution will allow the AHFC's identity theft prevention program to take effect immediately.

RESOLUTION No. AHFC _____ -__

BE IT RESOLVED BY THE BOARD OF DIRECTORS OF

THE AUSTIN HOUSING FINANCE CORPORATION:

WHEREAS, the Austin Housing Finance Corporation (AHFC) is a public non-profit corporation organized and operated under Chapter 394 of the Texas Local Government Code;

WHEREAS, AHFC has certain programs with specific eligibility requirements which provide loans to or on behalf of eligible persons, in order to promote safe, decent and affordable housing in the City of Austin. Any remaining balance existing on the maturity date of a loan is payable to AHFC on the loan's maturity date. These deferred payment loans qualify AHFC as a "creditor" under the Fair and Accurate Credit Transactions Act of 2003 ("FACTA");

WHEREAS, FACTA was enacted for the purpose of ensuring the preservation and protection of customer information by entities who possess such data for the purposes of billing for goods and services and extending lines of credit;

WHEREAS, the "Customer Privacy Assurance Program" contained within Exhibit "A" attached to this resolution represents AHFC's effort to ensure that all consumer data is comprehensively protected.

BE IT RESOLVED BY THE BOARD OF DIRECTORS OF THE AUSTIN HOUSING FINANCE CORPORATION:

The attached "Customer Privacy Assurance Program" of the Austin Housing Finance Corporation attached as Exhibit "A" is approved and adopted.

ADOPTED: _____, 2011 **ATTESTED:** _____

Shirley A. Gentry
Secretary

Exhibit "A"

Austin Housing Finance Corporation

Customer Privacy Assurance Program

OVERVIEW

Section 1: Program Overview

1.1: Purpose

The purpose of this program is to ensure the protection of consumer data and prevent identity theft. The Austin Housing Finance Corporation (AHFC) is committed to ensuring that no theft of customer information or other confidentiality breach occurs. If a breach does occur, AHFC will have policies and procedures in place to effectively address the issue with minimal inconvenience to the customer. The primary goal of this policy is to fuse existing policies, standard operating procedures and best practices in data protection in order to effectively address the purposes identified.

1.2: Scope

This program and companion policy applies to any individual or entity with an affiliation, direct or indirect, to AHFC. Affiliations with AHFC include, but are not limited to, employees (all classifications), contractors, vendors, customers or any other individual, entity, or agency using AHFC customer data for any purpose.

1.3: Administration

The Customer Privacy Assurance Program is administered by a Privacy Officer appointed by AHFC's General Manager. The Privacy Officer works with AHFC staff to ensure that this policy is uniformly implemented. These responsibilities may be delegated to a designee of the Privacy Officer.

1.4: Training

Any employee, vendor, contractor or other affiliate with access to AHFC customer information must be thoroughly trained. AHFC Privacy Officer is responsible for developing, implementing and revising standardized training courses which will be in full compliance with all relevant legislation. Foundational training standards will be established by the Privacy Officer.

1.5: Documentation

Each AHFC division is responsible for ensuring that all major identify theft events, as well as appropriate mitigation and resolution actions taken, are thoroughly documented on the appropriate logs and/or forms discussed in the "FACT Act Compliance Policies and Procedures".

1.6: Internal Reporting

The Privacy Officer will prepare an annual report of all major identity theft events, mitigations and resolution actions for the General Manager. Material changes made to the program as well as a statement of its overall effectiveness are also included in this report.

1.7: Reports to Consumer Reporting Agencies

In order to protect the privacy of AHFC's customers, information released to any external source regarding identity information must be limited. AHFC will provide notices of confirmed address updates to any Consumer Reporting Agency upon written request.

1.8: Program Review and Revision

The Privacy Officer meets semi-annually to review the status of the program and any corresponding policies. Members of AHFC's staff may solicit feedback from AHFC leadership and staff on key aspects of the policy which require revision. Recommendations for change are then made by AHFC staff to the Privacy Officer who must approve all revisions to the program and appropriate policies and procedures.

Section 2: Red Flags, Mitigation and Resolution

2.1: Overview of Identity Theft Red Flags

The Customer Privacy Assurance Program, and ancillary policies and procedures, are designed to detect, deter and prevent unauthorized access to consumer information and malicious account activity which might lead to identity theft. The following information discusses the specific "Red Flags" that agency policy addresses. A summary of actions to mitigate identify theft and resolve occurring incidents is also discussed.

2.2: Information from Consumer Reporting Agencies

AHFC may verify AHFC customer name(s) and demographic information using information from Consumer Reporting Agencies and third party sources as part of the new account establishment process. Information is obtained to verify the identity of a customer only.

Red Flag Warnings

1. A fraud or active duty alert is included with a consumer report.
2. A Consumer Reporting Agency provides a credit freeze on the customer report.
3. A Consumer Reporting Agency provides a notice of address discrepancy.
4. A consumer report indicates a pattern of activity that is inconsistent with the history and usual activity of a customer.

Summary of Mitigation

In order to mitigate possible identity theft under the provisions of these red flag warnings, AHFC will attempt to make contact with the customer and request additional documentation which substantiates identity prior to establishing a new account for the customer.

Summary of Resolution

If a customer or consumer reporting agency contacts AHFC concerning any of the possible warnings listed above, AHFC staff will verify the customer's identity and direct them to in-person service as necessary.

2.3: Suspicious Documents

During the application process, all customers for AHFC services or programs are required to produce certain standard types of documents in order to establish identity, residency and eligibility for the particular AHFC program being pursued. All identification documents must be unexpired.

Red Flag Warnings

1. Identification documents appear altered or forged.
2. The photo or physical description on the identification documents is not consistent with the appearance of the customer.
3. Other information given to open the account is not consistent with the identification documents provided by the customer.
4. Other information on identification documents is not consistent with readily accessible information on file such as signature or recent check
5. An application and/or supporting documentation appear to have been altered or forged, or give the appearances of having been destroyed or reassembled.

Summary of Mitigation

In order to mitigate the theft of a customer's identity under the possible red flag warnings defined in this section, AHFC staff will request additional documentation which can verify a customer's identity. If a customer is unable to produce additional documentation that verifies the customer's identity, no service, program or customer information may be established, modified or provided.

Summary or Resolution

If possibly fraudulent identification/documentation is submitted, AHFC staff will be trained on appropriate follow-up procedure. In certain cases, law enforcement may be contacted.

2.4: Suspicious Personal Identification (ID) Information

In addition to the physical documents required to establish an account for an AHFC service or program or to make changes to customer information, the following steps outline the process for addressing inconsistencies in the information submitted for the same purposes.

Red Flag Warnings

1. Personal ID is inconsistent with external information sources: addresses do not match consumer report/or social security number (SSN) has not been issued or is listed on the Social Security Death Master File [
2. Personal ID given by customer is not consistent with other personal ID info. (i.e.: There is a lack of correlation between the SSN range and DOB.)
3. Personal ID provided is associated with known fraudulent activity. Using the same addresses and/or phone number.
4. Personal ID is of the same type associated with fraudulent activity: fictitious address, mail box drop, or a prison; or phone number is invalid; it is associated with a pager or answering service.
5. The SSN is the same as customers opening other accounts.

6. The address or phone number is the same as a large number of other customers.
7. The customer fails to provide all needed personal ID information upon request.
8. Personal ID is inconsistent with utility records.
9. For institutions using challenge questions, the person attempting to access or open the account cannot provide any information beyond what would typically be found in a wallet or consumer report.

Summary of Mitigation

In order to mitigate the theft of a customer's identity under these possible red flag warnings, every effort is made to thoroughly and accurately confirm all information submitted. AHFC staff may request additional documentation which verifies the information provided by the customer. If a customer is unable to produce additional documentation that verifies the customer's identity, no program, service or customer account may be established or modified.

Summary of Resolution

If an identity theft event relating to one of the above listed red flag warnings does occur, specially trained AHFC staff will work with the customer to verify the accuracy of any identification information which AHFC has on file. In the event that a staff member suspects fraudulent information is being presented, AHFC may contact law enforcement if necessary.

2.5: Unusual Use or Suspicious Activity Related to the Covered Account

This section covers actions on existing accounts which may be considered fraudulent or malicious.

Red Flag Warnings

1. Change of billing address is followed by request for multiple changes to the account.
2. Payments are made in a manner associated with fraud. For example, deposit or initial payment is made and no payments are made thereafter.
3. Existing account with a stable history shows irregularities.
4. A covered account that has been inactive for a lengthy period of time is suddenly used.
5. Mail sent to customer is repeatedly returned.
6. Customer notifies utility that they are not receiving their bill.
7. AHFC is notified of unauthorized charges or transactions in connection with a customer's account.

Summary of Mitigation

AHFC staff is trained to notice possible irregularities in account information both on new and existing accounts. Addresses and identifying information are verified each time a customer contacts AHFC for any inquires or modifications to their account.

Summary of Resolution

If suspicious activity is reported by a customer, AHFC staff, or an outside entity, AHFC will immediately investigate the incident. Service on accounts with fraudulent activity will be immediately suspended until the investigation is fully resolved.

2.6: Notice of Theft

If AHFC is notified by law enforcement or other governmental agency that a fraudulent account has been opened or other malicious activity has occurred, staff should immediately take steps to comply with the orders of law enforcement.

Red Flag Warning
AHFC is notified by law officials or others, that it has opened a fraudulent account for a person engaged in identity theft.

Summary of Mitigation
If AHFC receives notification from law enforcement that it has opened a fraudulent account, service to the account will be suspended during investigation, and may ultimately be terminated.

Summary of Resolution
AHFC will comply with all orders and directions given by law enforcement.