

IDENTITY THEFT PREVENTION PROGRAM

COLDWELL BANKER-D'ANN HARPER REALTY PROPERTY MANAGEMENT
NOVEMBER 1, 2008

COLDWELL BANKER-D'ANN HARPER REALTY PROPERTY MANAGEMENT, located in SAN ANTONIO, TX 78258 developed the following Identity Theft Prevention Program to detect, prevent and mitigate identity theft in connection with the opening of a covered account, to ensure the program is updated periodically to reflect changes in risks or to the safety and soundness of the creditor from identity theft, and to fulfill the intent of the Identity Theft Red Flags Rule that implements section 114 of the Fair and Accurate Credit Transactions Act (FACT Act).

RED FLAGS RULE DEFINITIONS USED IN THIS PROGRAM

The Red Flags 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”.

“Covered Accounts” is defined as all mortgage applications and loans.

“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. This will include name, address, telephone number, social security number, date of birth, government issued driver’s license or identification number, alien registration number, government passport number, employer or taxpayer identification number.

IDENTIFYING RED FLAGS

Relevant red flags for the covered accounts were identified by reviewing incidents and methods of identity theft which has been evaluated to identify the following risk factors:

- Alerts, notifications, or other warnings received from consumer reporting agencies or service providers such as fraud detection services.
- The presentation of suspicious documents.
- The presentation of suspicious personal identifying information.
- The unusual use of, or other suspicious activity related to, a covered account.
- Notice from account holders, victims of identify theft, law enforcement authorities or other persons regarding possible identity theft in connection with covered accounts.

UPDATING THE IDENTITY THEFT PROGRAM

The Identity Theft Prevention Program will be reviewed and updated on an annual basis to reflect changes in risks to customers and the safety and soundness of our company from identity theft. In doing so, the Program Administrator will consider:

- The experiences of this company with identity theft.
- Changes in methods of identity theft.
- Changes in methods to detect, prevent and mitigate identity theft.
- Changes in the types of accounts this company offers or maintains.
- Changes in the business arrangements with other entities including mergers, acquisitions, alliances, joint ventures and service provider arrangement.

PROGRAM ADMINISTRATION

The Identity Theft Prevention Program is supervised by the Program Administrator who is responsible for:

- Assigning specific responsibility for the program's implementation.
- Reviewing staff reports regarding the detection of Red Flags.
- Reviewing steps for preventing and mitigating Identity Theft.
- Determining which steps of prevention and mitigation should be taken in particular circumstances.
- Annual evaluation and consideration of periodic changes to the Program.

STAFF TRAINING AND REPORTS

The Staff responsible for implementing the Program shall be trained either by or under the direction of the Program Administrator in the detection of Red Flags and steps to be taken when a Red Flag is detected. Staff will be required to submit to Program Administrator a written report on all incidents and suspicions of Identity Theft (SAR – Suspicious Activity Report), compliance with the Program and the effectiveness of the Program.

SERVICE PROVIDER ARRANGEMENTS

As applicable, any service provider engaged to perform an activity in connection with covered accounts, steps will be taken 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.

IDENTITY THEFT PREVENTION STEPS

COLDWELL BANKER-D'ANN HARPER REALTY PROPERTY MANAGEMENT
NOVEMBER 1, 2008

	RED FLAG IDENTIFICATION	APPLICABLE DETECTION STEPS ONE OR ALL MAY BE NECESSARY	PREVENTING & MITIGATING DETERMINE APPROPRIATE RESPONSE/S
CREDIT REPORTING AGENCY WARNINGS	Fraud Alert on Credit Report	Validate identifying information with external databases such as Fraud Guard	Notify the Program Administrator
	Active Duty Alert on Credit Report	Contact consumer if indicated to do so within the Fraud Alert or Activity Duty Alert	Determine that a Suspicious Activity Report (SAR) should be filed
	Alert - Name Discrepancy	Request additional identification documents	Refuse to proceed with application
	Alert - Address Discrepancy	Inspect identification document presented and verify it is government issued	Investigate other applications/accounts if applicable
	Alert - Social Security Number Discrepancy		Notify law enforcement
	Credit/Security Freeze on Credit Report		Determine that no response is warranted under the particular circumstances
	Deceased Indicator		
	Indication of inconsistent activity compared to customer's usual pattern		
	Inconsistent Social Security Number verification - Year and State Issued (SafeScan, Hawk or Fraud Shield)		

	RED FLAG IDENTIFICATION	APPLICABLE DETECTION STEPS ONE OR ALL MAY BE NECESSARY	PREVENTING & MITIGATING DETERMINE APPROPRIATE RESPONSE/S
SUSPICIOUS DOCUMENTS	Inconsistent Name on identification documents such as driver's license, social security card, etc.	Validate identifying information with external databases such as Fraud Guard	Notify the Program Administrator
	Inconsistent Address on identification documents such as driver's license, etc.	Request additional identification documents	Determine that a Suspicious Activity Report (SAR) should be filed
	Inconsistent Social Security Number on identification documents	Inspect identification document presented and verify it is government issued	Refuse to proceed with application
	Address or phone commonly associated with fraudulent activity, used by unusually large number of other persons, etc.		Investigate other applications/accounts if applicable
	Documents appear to be altered or forged		Notify law enforcement
	Photograph or physical description not consistent with applicant		Determine that no response is warranted under the particular circumstances

DISCLAIMER

The information contained in this document is not intended to be legal, accounting or other professional advice. Please consult with your legal or compliance advisor before taking any action on information contained in this document.