Identity Theft Red Flags

1. Policy Objective

The objective of this Policy is to implement the provisions approved by the Federal Reserve System, the Federal Deposit Insurance Corporation, the National Credit Union Administration, the Federal Trade Commission and the Department of Treasury's Office of the Comptroller of the Currency and Office of Thrift Supervision on detecting, preventing and mitigating identity theft for Greater Texas Mortgage ("the Company") business units that maintain Covered Accounts, as defined herein, or provide services related to the Covered Accounts of financial institutions or creditors.

2. Audience

This Policy applies to the Company. The Company reserves the right to change, modify, add or remove portions of this Policy at any time. Failure to comply with this Policy could result in consequences including, but not limited to, termination of employment.

3. Definitions

3.1 Red Flags

A pattern, practice or specific activity that indicates the possible existence of identity theft.

3.2 Identity Theft

A fraud committed or attempted using the identifying information of another person without authority.

3.3 Covered Account

An account primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions, or any other account for which there is a reasonably foreseeable risk to customers or the safety and soundness of the Company from identity theft.

4. Red Flags Program Requirements

The Company maintains Covered Accounts or provides services related to the Covered Accounts of financial institutions or creditors shall develop and implement a written Identity Theft Prevention Program appropriate to the nature, scope, size and complexity of the services provided to the financial institution or creditor (the "Program").

The Identity Theft Red Flags Program shall:

4.1 Identify which Identity Theft Red Flags are relevant to Greater Texas Mortgage.

4.2 Implement a process to detect the Identity Theft Red Flags applicable to maintaining or providing services to Covered Accounts.

4.3 Implement a process to provide appropriate responses to Identity Theft Red Flag triggers;

and

4.4 Periodically be updated to reflect changes that reduce customer risk.

5. Program Administration

Administration of the Program shall include the following:

5.1 Scott Yonce shall be responsible for the oversight, development, implementation, and administration of the Program;

5.2 Scott Yonce shall review annual reports regarding compliance with the requirements of the Program. The report will address the following:

5.2.1 The effectiveness of the Identity Theft Red Flags Policy;

5.2.2 Applicable service provider arrangements with third party vendors;

5.2.3 Significant identity theft incidents and management's applicable response; and

5.2.4 Recommendations for material changes to the Program; and approving material changes to the Program, as necessary, to address changing identity theft risks.

5.3 Implement training as necessary to effectively implement the Program; and

5.4 If a Company service provider is used in connection with Covered Accounts, the Company will ensure that the activity of the service provider is conducted pursuant to reasonable policies and procedures that are designed to detect, prevent and mitigate the risk of identity theft.

6. Audit and Enforcement of the Policy

Scott Yonce shall perform periodic audits of the compliance of this Policy.