SPECIAL BULLETIN 2008-10

September 30, 2008

TO: Retailers
Developers and Community Owners
Lenders
Manufacturers

FROM: Jess Maxcy

SUBJECT: **NEW** FTC Red Flag Rules
Deadline: November 1, 2008

As discussed during our September 18, 2008 Board of Directors' meeting, it has been determined that provisions of the Fair and Accurate Credit Transaction Act of 2003 apply to retailers who perform specific acts. (See attached MHI memo article.)

Thanks to the good work of MHI, our national association, compliance with the rule has been simplified by following the steps in the attached document. If you choose not to use the steps outlined, you may purchase compliance software from any number of companies on the internet. Simply type in "Red Flag Rules" on your search engine.

CALIFORNIA MANUFACTURED HOUSING INSTITUTE

Memorandum To: National Retailers Council

Date: September 10, 2008

Subject: FTC Red Flags Rule

The Federal Trade Commission (FTC) has issued regulations (the Red Flags Rule) requiring financial institutions and creditors to develop and implement written identity theft prevention programs as part of the Fair and Accurate Credit Transactions (FACT) Act of 2003. MHI believes that retailers who assist customers with applications for home loans are covered under the Red Flags Rule. In addition, retailers that are mortgage brokers are covered under the rule.

The programs must be in place by November 1, 2008 and must provide for the identification, detection, prevention, and response to activities known as "red flags" that could be indicators of identity theft. The Red Flags Identity Theft Prevention Program must enable a financial institution or creditor to:

1. Identify relevant patterns, practices, and specific forms of activity that are "red flags" signaling possible identity theft 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 from identity theft.

The rule states that the program developed must be appropriate to the size and complexity of the financial institution or creditor and the nature and scope of its activities. With this in mind, MHI has developed the attached document to assist retail sales centers in complying with the Red Flags Rule. The document includes the four areas listed above, plus a fifth area to document employee training on the program. In order to demonstrate compliance with the rule it is recommended that page one of the program document be placed in each consumer file noting any red flags that were identified.

Lastly, the rule requires oversight of the program by an employee at the level of senior management who will have the following responsibilities:

1. Assigning specific responsibility for the program's implementation

2. Reviewing reports prepared by staff regarding compliance at least annually
    a. Reports from staff should address material matters related to the program and evaluate issues such as: the effectiveness of the policies and procedures in addressing the risk of identity theft in connection with taking loan applications; significant incidents involving identity theft and management's response; and recommendations for material changes to the program
3. Approving material changes to the program as necessary to address changing identity theft risks.

FTC Business Alert

Federal Trade Commission ▪ Bureau of Consumer Protection ▪ Division of Consumer & Business Education

New 'Red Flag' Requirements for Financial Institutions and Creditors Will Help Fight Identity Theft

Identity thieves use people's personally identifying information to open new accounts and misuse existing accounts, creating havoc for consumers and businesses. Financial institutions and creditors soon will be required to implement a program to detect, prevent, and mitigate instances of identity theft.

The Federal Trade Commission (FTC), the federal bank regulatory agencies, and the National Credit Union Administration (NCUA) have issued regulations (the Red Flags Rules) requiring financial institutions and creditors to develop and implement written identity theft prevention programs, as part of the Fair and Accurate Credit Transactions (FACT) Act of 2003. The programs must be in place by November 1, 2008, and must provide for the identification, detection, and response to patterns, practices, or specific activities — known as "red flags" — that could indicate identity theft.

Who must comply with the Red Flags Rules?

The Red Flags Rules apply to "financial institutions" and "creditors" with "covered accounts."

Under the Rules, a **financial institution** is defined as a state or national bank, a state or federal savings and loan association, a mutual savings bank, a state or federal credit union, or any other entity that holds a "transaction account" belonging to a consumer. Most of these institutions are regulated by the Federal bank regulatory agencies and the NCUA. Financial institutions under the FTC's jurisdiction include state-chartered credit unions and certain other entities that hold consumer transaction accounts.

A **transaction account** is a deposit or other account from which the owner makes payments or transfers. Transaction accounts include checking accounts, negotiable order of withdrawal accounts, savings deposits subject to automatic transfers, and share draft accounts.

A **creditor** is any entity that regularly extends, renews, or continues credit; any entity that regularly arranges for the extension, renewal, or continuation of credit; or any assignee of an original creditor who is involved in the decision to extend, renew, or continue credit. Accepting credit cards as a form of payment does not in and of itself make an entity a creditor. Creditors include finance companies, automobile dealers, mortgage brokers, utility companies, and telecommunications companies. Where non-profit and government entities defer payment for goods or services, they, too, are to be considered creditors. Most creditors, except for those regulated by the Federal bank regulatory agencies and the NCUA, come under the jurisdiction of the FTC.

A **covered account** is an account used mostly for personal, family, or household purposes, and that involves multiple payments or transactions. **Covered accounts** include credit card accounts, mortgage loans, automobile loans, margin accounts, cell phone accounts, utility accounts, checking accounts, and savings accounts. A covered account is also an account for which there is a foreseeable risk of identity theft – for example, small business or sole proprietorship accounts.

Complying with the Red Flags Rules

Under the Red Flags Rules, financial institutions and creditors must develop a written program that identifies and detects the relevant warning signs — or "red flags" — of identity theft. These may include, for example, unusual account activity, fraud alerts on a consumer report, or attempted use of suspicious account application documents. The program must also describe appropriate responses that would prevent and mitigate the crime and detail a plan to update the program. The program must be managed by the Board of Directors or senior employees of the financial institution or creditor, include appropriate staff training, and provide for oversight of any service providers.

How flexible are the Red Flags Rules?

The Red Flags Rules provide all financial institutions and creditors the opportunity to design and implement a program that is appropriate to their size and complexity, as well as the nature of their operations. Guidelines issued by the FTC, the federal banking agencies, and the NCUA (**ftc.gov/opa/2007/10/redflag.shtm**) should be helpful in assisting covered entities in designing their programs. A supplement to the Guidelines identifies 26 possible red flags. These red flags are not a checklist, but rather, are examples that financial institutions and creditors may want to use as a starting point. They fall into five categories:

- alerts, notifications, or warnings from a consumer reporting agency;
- suspicious documents;
- suspicious personally identifying information, such as a suspicious address;
- unusual use of — or suspicious activity relating to — a covered account; and
- notices from customers, victims of identity theft, law enforcement authorities, or other businesses about possible identity theft in connection with covered accounts.

More detailed compliance guidance on the Red Flags Rules will be forthcoming. For questions about compliance with the Rules, you may contact **RedFlags@ftc.gov**.

The FTC, the nation's consumer protection agency, works to prevent fraudulent, deceptive, and unfair business practices in the marketplace and to provide information to help consumers spot, stop, and avoid them. To file a complaint or to get free information on consumer issues, visit ftc.gov or call toll-free, 1-877-FTC-HELP (1-877-382-4357); TTY: 1-866-653-4261. The FTC enters Internet, telemarketing, identity theft, and other fraud-related complaints into Consumer Sentinel, a secure online database available to hundreds of civil and criminal law enforcement agencies in the U.S. and abroad.

Your Opportunity to Comment

The National Small Business Ombudsman and 10 Regional Fairness Boards collect comments from small businesses about federal compliance and enforcement activities. Each year, the Ombudsman evaluates the conduct of these activities and rates each agency's responsiveness to small businesses. Small businesses can comment to the Ombudsman without fear of reprisal. To comment, call toll-free 1-888-REGFAIR (1-888-734-3247) or go to www.sba.gov/ombudsman.

Federal Trade Commission	ftc.gov
1-877-FTC-HELP	For The Consumer

June 2008

Red Flags Identity Theft Prevention Program

Step 1	Identify relevant patterns, practices, and specific forms of activity that are "red flags" signaling possible identity theft. Use any incidents of identity theft experienced at the retail sales center in the past to help identify sources of "red flags."

List of Possible "Red Flags"

Alerts, Notifications or Warnings from a Consumer Reporting Agency

1. A fraud or active duty alert is included with a consumer credit report
2. A consumer reporting agency provides a notice of credit freeze in response to a request for a consumer report
3. A consumer reporting agency provides a notice of address discrepancy that informs you of a substantial difference between the address used to request the consumer report, and the address(es) in the agency's file for the consumer
4. A consumer report indicates a pattern of activity that is inconsistent with the history and usual pattern of activity of an applicant or customer such as: 1) a recent and significant increase in the volume of inquiries; 2) an unusual number of recently established credit relationships; 3) A material change in the use of credit especially with respect to recently established credit relationships; and 4) an account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor.
5. Documents provided for identification appear to have been altered or forged
6. The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification
7. Other information on the identification (i.e. address, date of birth) is not consistent with information provided by the person opening a new covered account or customer presenting the identification

Suspicious Personal Identifying Information

1. Address does not match any address in the consumer credit report
2. The Social Security Number has not been issued, or is listed on the Social Security Administration's Death Master File
3. 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
4. The customer fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete
5. Documents or information supplied appear to be forged or altered or destroyed and reassembled
6. Customer unable to answer personal information correctly when challenged
7. Information on ID such as signature is inconsistent with information on file or from document to document

Suspicious Activity From Past Experience That Indicates Possible Identity Theft

1.
2.
3.
4.

Step 2	Detect and note "Red Flags" that have been identified	Step 3	Response to "Red Flag" Identified
Example: Address provided by customer does not match any address in consumer credit report		Example: Verify the customer's identity by requesting additional documents such as a social security card to match with the S.S.N. on the credit report or a current utility bill showing the customer's current address	
1.		1.	
2.		2.	
3.		3.	
4.		4.	
5.		5.	
6.		6.	

Red Flags Identity Theft Program Compliance Records

Step 1 Review and Update the Red Flags Identity Theft Program periodically to reflect changes in risks from identity theft as needed.

Mo./day/yr. of review	Make Note of Changes or Updates to Your Red Flags Identity Theft Program

Step 2 Train staff, as necessary, to effectively implement the Red Flags Identity Theft Program

Date	Employees Trained	Notes on Training