Identify Theft Policy
Red Flags and Discrepancies Under the FACT Act of 2003

STATEMENT

Having determined that the request for a written policy concerning "Identity Theft Red Flags and Address Discrepancies under the FACT Act of 2003(know as the FACT Act)" applies to mortgage loans, mortgage brokers and in specific, Marvel Ventures Mortgage, Inc. (MVMI), the following policy is implemented to take effect November 1, 2008. (Re: "Some specific examples of covered accounts cited in the rule include: credit card accounts, "mortgage loans", automobile loans, margin accounts, cell phone accounts, utility accounts, checking accounts, and savings accounts" of the "Identity Theft Red Flags & Address Discrepancies under the FACT Act of 2003.")

Since "mortgage loans" has been identify in the "ACT", this written policy is being implemented because of a direct study of the Identity Theft laws, the current policies, and practices of Marvel Ventures Mortgage, Inc. moreover, its need to be in compliance. Having examined and evaluated all aspects of possible "Identity Theft and Address Discrepancies" to determine our practices and need for the written policy, the Board of Directors of Marvel Ventures Mortgage, Inc. has approved of this written policy. This policy is being implemented and enforced on November 1, 2008.

While this new written policy is replacing some our practices and enhancing/amending others, understand that Marvel Ventures Mortgage, Inc. has always practice good identify theft protection for our clients.

This written policy will be strictly, adhered to so as ensure that Marvel Ventures Mortgage, Inc. is always in compliance with the FACT Act.

Prelude

Marvel Ventures Mortgage, Inc., while completing the "Study", considered the following:

1.The types of covered accounts it maintains;
2.The methods it provides to open its accounts;
3.The methods it provides to access its accounts;
4.Its previous experience with identity theft.

Marvel Ventures Mortgage, Inc has always practiced good management of a client's private and personal information. Each client, who provides the appropriate information, is protected whether they continue seeking service with MVMI or chose not to complete their business with MVMI. All client information that is computer generated is protected by encrypted, secure sites and the information can only be accessed by authorized personal, with password protection assigned by the Owner and President of Marvel Ventures Mortgage, Inc. The administrative supervisor protects any information, which is printed or documented, in locked, secure storage areas.

To further, protect the client, MVMI uses an "Opt-Out" database to protect the client's right to privacy and possible identity theft. This is always completed prior to performing a credit check so the client will not have their privacy violated in any way. The National Association of Mortgage Brokers (NAMB) has advised mortgage brokers that "opting out" procedures must be preformed within five (5) minutes of the/any credit review or the

client's information and scores will be distributed as credit bureaus so choose and the list can be in the hundreds.

The following guidelines were used in preparing and writing a policy for establishing and maintaining an Identity Theft Prevention Policy and Practices:

This written policy includes reasonable policies and procedures to address the risk of identity theft posed to its clients or its own safety and soundness. These written policies must address financial, operational, compliance, reputation, and litigation risks, and should be designed to the size and complexity of mortgage brokers, in general, or client and the nature and scope of its activities. MVMI has used the detailed guidance in Appendix J of the final rule. MVMI designed their policies in accordance with information provided in Appendix J and include in its written polices those guidelines it deems appropriate. However, MVMI did not used suggestions in Appendix J, which are not appropriate for our current operations.

The guidelines in Appendix J, also, make it clear that MVMI must follow "Identity Theft Red Flags and Address Discrepancies" under the FACT Act of 2003. MVMI, by the new rule may, where appropriate, incorporate into its written policy existing processes for controlling reasonably foreseeable risks of identity theft.

Marvel Ventures Mortgage, Inc has incorporated the four basic elements that must be included in the written policy.

They are the following:

1. Identifying relevant Red Flags for clients, and incorporating those Red Flags into the written policy:

   a."Red Flags" are defined as any pattern, practice, or specific activity that indicates the possible existence of identity theft.
   b.Red Flags should be identified and incorporated from relevant sources including:
      i. Prior incidents of identity theft that the mortgage broker or client has experienced;
      ii. New methods of identity theft that MVMI has identified as reflective of changes in identity theft risks; and
      iii. Applicable supervisory guidance.

   c. When identifying Red Flags, mortgage brokers must consider the nature of their business and the type of identity theft to which they may be subject.

2. Detecting Red Flags that have been incorporated into the written policy:

   a.The new rules suggest mortgage brokers should enhance their ability to detect Red Flags incorporated in their written policies by, among other things:

      i. Verifying the identity of individuals opening covered accounts;
      ii. Authenticating the identity of customers with existing accounts;
      iii. Verifying the validity of change of address requests.

3. Responding appropriately to any Red Flags that are detected to prevent and mitigate identity theft;

   a. In determining the appropriate response to Red Flags that are detected by the written policies, mortgage brokers should consider any aggravating factors that may heighten the risk of identity theft (examples of such factors are outlined in Section IV of the guidelines included in Appendix J- Identity Theft Red Flags and Ad-

dress Discrepancies under the FACT Act of 2003.)
Identify Theft Policy
Red Flags and Discrepancies Under the FACT Act of 2003
(continued)

4. Ensuring the written policy is updated periodically to reflect changes in risks to clients or to the safety and soundness of MVMI from identity theft.

a.Section V of the guidelines included in Appendix J identifies several factors that should cause a mortgage broker to update its written policy, including:

i. The mortgage broker's own experience with identity theft;
ii. Changes in methods of identity theft;
iii. Changes in methods of detecting, preventing, or mitigating identity theft;
iv. Changes in the types of information the MVMI maintains; and
v. Changes in MVMI's business practices.

Administration of the Identity Theft Written Policy:

The new rule also requires mortgage brokers to take certain steps in administrating the written policy.

These steps include:

1.Obtaining approval of the initial written policy from their Board of Directors or a Committee of their Board of Directors:

a.For mortgage brokers, that do not have a Board of Directors, approval must be obtained from a designated employee at the level of senior management. Marvel Ventures Mortgage, Inc has a Board of Directors.

2.Ensuring oversight of the development, implementation, and administration of the written policy;

a.The final rule states that oversight should include:

i. Assigning specific responsibility for the written policy's implementation;
ii. Reviewing reports, prepared at least annually, by staff concerning the compliance of the mortgage broker with new rules;
iii. Approving material changes to the written policy as necessary to address changing identity theft risks will only be done by the owner/president of Marvel Ventures Mortgage.

3.Training staff:

a.Each mortgage broker to whom the new rules apply must train members of their staff, as necessary, to effectively implement the written policy.

b.Training is required only for "relevant staff." However, the term "relevant staff" is not further defined Identity Theft Red Flags & Address Discrepancies under the FACT Act of 2003

4.Overseeing Service Provider arrangements:

a.Each mortgage broker, to whom the new rules apply, must exercise appropriate and effective oversight of Service Provider arrangements.

b.The guidelines included in Appendix J explain that whenever a mortgage broker engages a Service Provider to perform an activity in connection with a client, the mortgage broker must ensure that the activity of the Service Provider is conducted in accord with reasonable policies and procedures for detecting, preventing, and mitigating the risk of identity theft.
Identify Theft Policy

c.The guidelines in Appendix J also provide an example of how a mortgage broker may comply with this requirement of the rule.

i.A mortgage broker could require their Service Providers, by contract, to have policies and procedures in place to detect relevant Red Flags that may arise in the performance of their activities. These Service Providers could further be required to either report these Red Flags to the mortgage broker or take the necessary and appropriate steps to prevent or mitigate identity theft.

Thus the creation of the 'written policy and practices' for Identity Theft Red Flags and Address Discrepancies are established by Marvel Ventures Mortgage, Inc. and the effective date of this written policy is November 1, 2008. The following document is the written policy in compliance with the "FACT Act of 2003".

Identify Theft Policy
Red Flags and Discrepancies Under the FACT Act of 2003
As It Applies To
Marvel Ventures Mortgage, Inc.
November 1, 2008

Scope:

Marvel Ventures Mortgage, Inc. (MVMI), completed a "Study" on identify theft and red flags for discrepancies, considered the following:

1.The types of covered accounts it maintains;
2.The methods it uses to review a client's personal and private credit information;
3.The methods it provides to access its client's credit information;
4.Its previous experience with identity theft.

The following written policy was developed as a direct result of that study, using the above guidelines. This policy is effective November 1, 2008.

Policy:

Initial Contact Policy:

MVMI has many forms of initial contact with a potential client. They are the following:

1.Telephone Call-in (the most popular)
2.E-mail

3.Walk-in

“However, all clients that identify themselves and do business with Marvel Ventures Mortgage, Inc, in any way, are considered “Covered Clients” and their personal information is protected and strictly held confidential. At NO time is any client information share with anyone, internally or externally, that does NOT have a need to know.

Each type of client contact has procedures that the staff follows. (1. Identifying relevant Red Flags for clients,)

Telephone Call-In (Initial contact):

As a telephone call comes in, and a potential client is identified, the red flag process begins.

1.All clients are given a “Client Evaluation Sheet” treatment. Before any client information is taken, a ‘disclosure statement’ is read to them that assures them of their right to privacy and accuracy of their information. At no time is their results of a credit review shared with anyone other that the actual (potential) client.

2.No information is given over the telephone on the first call. All (potential) clients are called back and asked to identify themselves appropriately.

3.However, if the credit report agency provides a report of (potential) client that has an Identify Theft Alert in whether, it be an “Initial alert’ or an ‘extended alert’ more stringent steps are take to identify the (potential) client and absolutely no information is given out until their identity is verified and verified without question to their identity.
Identify Theft Policy
Red Flags and Discrepancies Under the FACT Act of 2003
As It Applies To
Marvel Ventures Mortgage, Inc.
November 1, 2008
(continued)

E-mail

4.E-mail requests are responded to initially with an email back. But again, once a (potential) client is established, all further contact with that person is either by telephone or in person so as to follow the policy and procedures in the above steps for “identity theft’.

Walk-In

5.Walk-ins seeking information. The policy and procedure is simple. They must prove through a picture id and social security number verification before a (potential) Client Evaluation Sheet is completed.

6.When the client provides with the correct identification and a Client Evaluation Sheet is completed. The following procedure is followed:

a.The (potential) client’s information is entered in an “Opt-Out” prescreen database. After the accepted form is shown and printed with a copy given to the (potential) client, then and only then,
b.Is the (potential) client’s information is entered into a Credit Review database. “TransUnion” credit bureau

is only bureau accessed to obtain initial credit information. After a review of the report by a certified FCRA person to ensure that there are no fraud alerts and/or multiple social security numbers then that information is shared with the (potential) client.
c.However, If there is any questions of identity, alerts or red flags, the following action is taken:

i.Reexamine all identification to ensure proper matching of numbers.
ii.Advise client of problem
iii.Take appropriate action for situation

d.A written course of action will be attached to that file and stored for the State mandated amount of time.

e.If any legal action is determined necessary, Marvel Ventures Mortgage, Inc will take the appropriate action at that time.

NON CLIENTS

Any information that is retained, even though an individual does not become a client, has their personal and private information filed in non public areas and/or stored in secure filing areas.

ACTIVE FILES

All files that are considered active are handled as follows:

1.Initial information is gathered and screened to establish that the individual has the possibility of obtaining a mortgage loan.

2.All materials are put away from any possible public contact and/or viewing before the client makes their initial contact with the Loan Officer.

3.As the Loan Officer uses and gathers further information about a client, that information is put in a file folder and kept in a secure non public area when not in use. At all times, as New information is gather, the Loan Officer and Loan Processor is checking for any Red Flags for improper matching of information to the client.

4.As the file is given to the Loan Processor, again the client's folder is only kept on top of their desk when being processed for a loan. The Loan Processor always maintains complete secure holding of a file at all times.

5.When a file receives a "Clear-To-Close" (CTC) designation and is passed to the Office Administrator. It is passed in a completely contained folder and only on that person desk as the proper paperwork for finally closing is prepared. But never viewed by any else, except those that are involved in the "Closing Process" and always kept in a non public area when not working on that file for closing purposes.

FINAL STORAGE

As a client completes the closing process and a file becomes closing. That file is placed in a secure, locked file cabinet, along with other pertinent documents, for the State mandated term of three 3 years.

At any time, a review of a client's file is necessary, that review may be performed by, only, individuals with a

‘need-to-know’ and then returned to the secure, locked file cabinet.

One Final Comment: Should any questions arise or any information unclear, it always double and triple checked and brought to the attention of the most senior management for review and disposition.