APPENDIX IIIC -IDENTITY THEFT PREVENTION PROGRAM (Red Flag Rules)

POLICY AND PROCEDURES

MDA Insurance & Financial Group, Inc.

Effective Date: May 1, 2009

I. PURPOSE

The purpose of this policy is to establish procedures to follow to protect customer financial information in compliance with the Red Flag Rules issued pursuant to the Fair and Accurate Credit Transactions Act.

II. POLICY

It is the policy of MDA Insurance and Financial Group to identify and detect relevant patterns, practices, and activities that are Red Flags indicating possible identity theft, to respond appropriately to those Red Flags, and to correct or mitigate the harm suffered by any person whose information is used unlawfully.

III. DEFINITIONS

A. Covered Account

A covered account is 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 our customers of identity theft. An account includes any extension of credit, such as the deferred payment of insurance premiums, amounts due for products we distribute and services we provide.

B. Identifying Information

Identifying information includes a person's first and last name in combination with any information that could be used to access a person's financial resources, including but not limited to, the person's Social Security Number, driver's license, passport, state identification card, bank account numbers, credit card numbers, personal identification numbers, and passwords. Also included would be an entity's name in combination with its taxpayer identification number, corporate identification number, address, etc.

C. Red Flags

Red flags are patterns, practices, and activities that indicate possible identity theft.

D. Security Breach

A security breach occurs when an unauthorized person/entity gains access to a customer's identifying information, where the information is used or intended to be used for an unlawful purpose.

IV. PROCEDURES

A. Identification of Red Flags

The following is a list of Red Flags that we must look for during daily operations. Each of us has been given a copy of this program and shall keep a copy in his or her work area for reference.

1. A fraud or active duty alert that is included in a customer's consumer 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.

4. A consumer report indicates a pattern of activity that is inconsistent with the history and usual patter of activity of a customer, such as:

    a. A recent and significant increase in the volume of inquiries;

    b. An unusual number of recently established credit relationships;

    c. A material change in the use of credit, especially with respect to recently established credit relationships; or

    d. 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 by a customer appear to have been altered or forged.

6. The photograph or physical description on identification presented by customer is not consistent with the appearance of the customer.

7. Information we obtain to identify a corporate or other customer is inconsistent with information provided by the customer.

8. Other information on the identification is not consistent with readily accessible information that is in our files, such as a signature card or a recent check.

9. Documents that appear to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

10. Identifying information provided is inconsistent when compared against external information. For example:

    a. The address does not match any address in the consumer report; or

    b. The Social Security Number (SSN) has not been issued, or is listed on the Social Security Administration's Death Master File. The following numbers indicate an invalid SSN:

        i. The first three digits are 000, 666, are above 77s, or are in the 800 or 900 range.

        ii. The fourth and fifth digits are 00.

        iii. The last four digits are 0000.

11. Identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the practice. For example:

    a. The address on an application is the same as the address provided on a fraudulent application; or

    b. The phone number on an application is the same as the number provided on a fraudulent application.

12. Identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by us. For example:

    a. The address on an application is fictitious, a mail drop, or a prison; or

    b. The phone number is invalid, or is associated with a pager or answering service.

13. The SSN, taxpayer identification number, corporate identification number or other identification provided is the same as that submitted by other persons opening an account or other customers.

14. The address or telephone number provided is the same as or similar to the account number or telephone number submitted by an unusually large number of other persons opening accounts.

15. The personal opening the account fails to provide all required identifying information on an application or in response to notification that the application is incomplete.

16. The person opening the covered account or the customer cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.

17. A covered account is used in a manner that is not consistent with established patterns of activity on the account. For example, nonpayment when there is no history of late or missed payments.

18. Mail sent to a customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's covered account.

B. Detection of Red Flags

To detect the Red Flags listed above, we should consider procedures to verify the identity of each customer:

1. Obtaining identifying information about, and verifying the identity of, a person or entity opening an account.

2. Authenticating the information obtained regarding a customer's identity and monitoring customer transactions and verifying the validity of change of address requests and other changes to identifying information.

3. Follow other procedures necessary to form a reasonable belief that we know the true identity of each customer.

4. Obtaining for individual customers the following:

    a. Name;

    b. Date of birth;

    c. Address

5. For corporation or other entity:

    a. The address of the principal place of business, local office or other physical location;

    b. An identification number (i.e. a taxpayer identification number, corporate identification number, etc.)

C. Appropriate Response to Red Flags

The following are actions that we must take when a Red Flag is detected.

1. A staff member who detects a Red Flag should immediately notify his or her supervisor.

2. Any time a Red Flag is detected, the supervisor must mark the customer account associated with that Red Flag accordingly. Every customer account with a Red Flag will be monitored for a period of one year.

3. The Program Administrator must investigate any Red Flag to determine whether the detection could possibly result in the misuse of identifying information. If so, then the Program Administrator will take the following actions.

    a. The Program Administrator must notify the customer in writing of the Red Flag, provide a summary of the incident, and advise the customer to monitor free credit reports and possibly contact the major credit reporting agencies.

    b. The Program Administrator may close the customer's account, reopen the customer's account with a new account number, and change any passwords or security codes associated with the account.

    c. If necessary, the Program Administrator may elect to notify local law enforcement.

4. If a customer notifies us of possible identity theft associated with the customer's account, the Program Administrator must investigate the claim and attempt to mitigate any harm.

    a. The Program Administrator must notify the customer in writing of the Red Flag, provide a summary of the incident, and advise the customer to monitor free credit reports and possibly contact the major credit reporting agencies.

    b. Once the customer's claim is verified, we will cease any collection activities into the account.

    c. If the identity theft resulted in an adverse report made to a consumer reporting agency in association with the customer account, the Program Administrator will notify the consumer reporting agency that the account was not the customer's responsibility.

    d. If necessary, the Program Administrator may elect to notify local law enforcement.

e. If the Program Administrator determines that the customer has not been the victim of identity theft, the Program Administrator will advise the customer in writing of the basis for that determination and that the customer is responsible for the payment of the account.

D. Staff Training

The Program Administrator will develop a training program to educate staff members on the importance of identity theft, how it can affect us and our customers and how to comply with the Identity Theft Prevention Program policy and procedures.

E. Periodic Update of the Identity Theft Prevention Program

The Program Administrator will reassess the program on an annual basis to determine whether any changes should be implemented. The Program Administrator will consider such factors as any incidents of identity theft that have occurred, changes in our business such as updated technology or new types of covered accounts, changes in methods of identity theft, and changes in methods of detecting and preventing identity theft. The Program Administrator shall periodically submit a report to the Board of Directors that documents any significant identity theft incident(s) that have occurred, any changes in risk to our customers, and recommendations to improve the program. The Board must approve all changes made to the program.