

RED FLAG RULES

Identity Theft Prevention Program

October 26, 2009

MedChi has approved this Identity Theft Prevention Program (Program), developed to comply with the Federal Trade Commission's (FTC) Identity Theft Prevention Red Flag Rules (16 CFR § 681.2). This mandated written Program outline has been prepared by MedChi's Law & Advocacy Division, in consultation with various divisions within MedChi.

I. Definitions

For purposes of the Program, the following terms are defined as follows:

“Creditor” means any entity that regularly extends, renews or continues credit, including but not limited to transactions in which payment is deferred or deferred payment is accepted.

“Covered Account” means any account that a creditor offers or maintain that is used primarily for personal family or household purposes, that involves multiple payments or transactions. A covered account also includes any other account that the creditor offers or maintains for which there is a reasonably foreseeable risk to customers from identity theft.

“Identity Theft” means fraud committed using the identifying information of another person.

“Red Flag” means a pattern, practice, or specific activity that indicates the possible existence of identity theft.

II. Purpose

The purpose of the written Program is to accomplish the following:

- a) Identify potential Red Flags based on risk factors associated with covered accounts;
- b) Formulate policies and procedures to detect Red Flags;
- c) Prepare and implements steps to be taken to prevent, detect, identify and mitigate identity theft;

- d) Institute administrative measures to provide oversight and updating of the written Program.

III. Identification of Red Flag

Presentation of any of the following issues constitutes a Red Flag:

- suspicious document or personal identifying information
- prior incidence(s) or knowledge of methods of potential or actual identity theft, or the compromising of personal identifying information
- unusual activity or practices relating a covered account
- alert(s) or information discovered or received from others

IV. Detection of Red Flag

Detection of the Red Flag(s) identified, steps to be taken to obtain and verify the identity of an individual are the following:

- Obtain identifying information and verify as appropriate and necessary;
- Verify any change in address, billing information, or credit card information;
- Verify the identity of the individual with whom you are speaking or obtaining information, prior to your release of any personal and/or identifying information.

V. Prevention and Mitigation of Identify Theft

Monitor and secure covered accounts to prevent and detect, as indicated, circumstances of potential identity theft. If detected or suspected, appropriate measures should be in place and exercised to address the source, notify the individual where indicated, and work toward mitigating and/or resolving the risk. Identification of the necessary elements to prevent, detect, identify and mitigate possible situations of identify theft are included in this step of the written program. Incorporation of existing policies and procedures that control reasonably foreseeable risks of identity theft should necessarily be included in the written Program.

In response to an incident of identity theft, the following steps should but not be limited to the following:

- An affidavit executed by the individual affected by the personal identifying information having been compromised (see attached);
- The account that has been compromised closed;
- A new covered account established for the individual;

-Measures taken to ensure that the victim of identity theft is not held responsible for financial charges associated with the incident;

-Report(s) made to the proper authorities regarding the incident.

VI. Program Administration

Pursuant to the FTC Red Flag Rules, 16 CFR Part 681.2(e), there must be continued administration of the Program by a designated senior level administrator. This designated individual is responsible for oversight, development, implementation and ongoing administration of the Program. Staff for your division is to be trained as necessary in order to effectively implement, continue and ensure ongoing success of the Program. Initial approval of the written Program by senior level administration is required in the absence of a board of directors.

VIII. Program Updating

The Administrator is responsible for ensuring periodic review of the Program to ensure that it incorporates potential or actual incidences of identity theft that have occurred since the prior review as well includes other appropriate updates to bring it current. During each review, the effectiveness of the Program should be considered, including but not limited to any changes in risks of identity theft of covered accounts and incidences that have occurred relating to potential or actual prevention, detection, identification and mitigation of identity theft.