Attorneys and Counselors

ELMS ♦ HARMON ♦ MACCHIA

A Limited Liability Company
www.elmslaw.com

7800 I.H. 10 West, Suite 600
San Antonio, Texas 78230-4754
Lee Elms

Telephone (210) 349-8888
Facsimile (210) 349-8805
l.elms@elmslaw.com

RED FLAGS RULE

The Federal Trade Commission has issued a regulation known as the Red Flags Rule ("Rule"). This regulation is aimed at guarding against identity theft by protecting confidential personal information found in *credit reports*, *credit applications*, and *any other document containing sensitive personal information*. This letter will provide a brief discussion of responsibilities under the Red Flags Rule.

In order to determine if the Rule applies to your company you must first decide if your company is a financial institution or a "creditor." Under the Rule, a creditor includes businesses or organizations that regularly defer payment for goods or services or provide goods or services and bill customers later. The Rule also defines a "creditor" as one who regularly grants loans, arranges for loans or the *extension of credit*, or *makes credit decisions*. In addition, the definition also includes anyone who regularly participates in the decision to extend, renew or continue credit. For example, if a company offers its own credit card, arranges credit for its customers, or *extends credit by selling customers goods or services and billing them later it is considered a creditor under the Rule.*

Once you have concluded that your business or organization is a creditor, you must determine if you have any "covered accounts" as defined by the Rule. There are two categories of "covered accounts." The first is a consumer account you offer your customers that is primarily for personal, family or household purposes that involves or is designed to permit multiple payments or transactions. The second kind of account covered by the Rule is any other account that a creditor offers or maintains for which there is a *reasonably foreseeable* risk to customers or to the safety and soundness of the creditor from identity theft including financial, operational, compliance, reputation, or litigation risks. Examples of the second kind of "covered accounts" include small business accounts or sole proprietorship accounts. In determining if your accounts are covered under this second category, you should consider how the accounts are opened and accessed. If your accounts are accessed remotely, such as through the Internet or by telephone, there may be a reasonably foreseeable risk of identity theft.

If you determine you are a creditor, the Rule states you must periodically determine whether you offer or maintain one of these "covered accounts" by conducting a periodic risk assessment. As part of this assessment, you should take into account (1) the method in which you open accounts, (2) the method in which you provide access to the accounts and (3) your previous experience with identity theft.

Should you determine that you are a creditor with "covered accounts," the *Rule requires you to develop and implement a written Identity Theft Prevention Program that is designed to prevent, detect, and mitigate identity theft in connection with the opening of new accounts and the operation of existing ones.* The program must be appropriate for the size and complexity of your business and you must designate an employee of senior management to be responsible for the oversight and administration of the program as well as train support staff who handle this sensitive information. Your program must identify the red flags of identity theft, set up procedures to detect those red flags in your day-to-day

operations, respond appropriately to the red flags to prevent and mitigate the harm done, and update your program often to adapt to the rapidly changing risks of identity theft.

Some of the potential problems that are often seen and could be considered risks are:

(1) who has access to credit reports and account information
(2) is the information secure (locked or protected) at all times
(3) who has access to sensitive information stored on databases (i.e., are only the last four numbers of a social security number displayed or can all employees view a customer's entire social security number), and;
(4) what electronic protection methods are used for electronically stored information.

According to the definition found in the Red Flags Rule, you may be a creditor.

In order to determine if your company offers or maintains any accounts for which there is a *reasonably foreseeable* risk to customers or to the safety and soundness of the creditor from identity theft, you may wish to consider contacting an expert in identity theft to conduct the required periodic risk assessment. If it is determined that there are reasonably foreseeable risks that could expose your business and/or your customers to identity theft, then I recommend you work with an expert in identity theft to develop a written Identity Theft Prevention Program that is in compliance with the Red Flags Rule.

DISCLAIMER: The content in this article is intended for general information purposes only, and *is* *not* legal advice. Legal advice depends on the specific facts and circumstances of each individual's situation. Those seeking specific legal advice or assistance should contact an attorney.