BUTZEL LONG
ATTORNEYS AND COUNSELORS

Technology and E-Commerce E-news

October 30, 2009

RED FLAG the Red Flag Rules: Effective Date: November 1, 2009

If your business provides goods or services and you bill your customers for those goods and services, you are a "creditor" subject to the new Red Flag Rules ("Rules") designed to prevent identity theft. The intent of the Rules is to prompt creditors to go into "authentication mode" and determine whether fraudsters are trying to apply for credit in someone else's name or hijack someone else's accounts. To comply, your business must develop and implement identity theft prevention programs. Failure to comply could result in penalties of up to $2,500 per "knowing violation."

The Federal Trade Commission (FTC), the federal bank regulatory agencies, and the National Credit Union Administration jointly issued regulations called the "Red Flag Rules" on November 9, 2007.[1] Their effective date has been deferred numerous times but they are scheduled to go into effect on November 1, 2009.

The Rules require financial institutions and creditors to implement programs to detect, prevent, and mitigate identity theft in connection with new and existing accounts. These Rules apply to all individuals and organizations that meet the definition of "creditor" if the organizations offer or maintain "covered accounts". "Covered accounts" are defined as (1) an account primarily for personal, family or household purposes that involves or is designed to permit multiple payments or transactions or (2) any other account for which there is a reasonably foreseeable risk to customers or the safety and soundness of the financial institution or creditor from identity theft.

A Red Flag is "any pattern, practice or specific activity indicating potential identity theft." There are 26 examples of suspicious behavior that creditors can use as red flag guidelines in five general categories of red flags:

- Alerts, notifications or warnings from a consumer reporting agency
- Suspicious identification documents, such as the presentation of an altered document
- Suspicious personal identifying information, such as a suspicious Social Security number, address change or a photograph on an ID that is inconsistent with appearance of person presenting the ID
- Unusual use of an account or other dubious account-related activity, such as a credit freeze

- Notices from customers, victims of identity theft, law enforcement authorities or other persons regarding possible identity theft in connection with your accounts, such as a fraud alert on a credit report

The Rules have an unexpectedly broad application because the definition of "creditor" includes any entity that (i) extends, renews or continues credit; (ii) arranges for someone else to extend, renew or continue credit; or (iii) is the assignee of a creditor who is involved in the decision to extend, renew or continue credit. For example, if an individual or business regularly offers payment plans or allows customers to pay for goods or services in installments, the organization would be considered a "creditor" within the meaning of the Rules. Many organizations that typically do not think of themselves as "creditors" are, including individuals and organizations that defer payment for goods or services including governmental entities.

In addition to banks, there are other financial institutions and stores that sell on credit. Below are some examples of atypical creditors where payment is made after the product was sold or the service was rendered:

- Schools that extend credit to students, or parents of students, through institutional loan programs, retail installment contracts or deferred payments plans;
- Hospitals and physicians who bill their patients for copayment and coinsurance or who allow patients to pay their bills over time through payment plans;
- A non-profit or government agency, that accepts deferred payments for goods or services, such as a municipal water or sewer services.

Your business must develop and implement a written identity theft prevention program that is:

- Designed to detect, prevent and mitigate identity theft in connection with its covered accounts
- Appropriate to the size and complexity of your business and the nature and scope of its activities.

There is no "one size fits all" for compliant identity theft prevention programs; however, all programs must:

- Identify red flags a creditor may come across in day-to-day operations;
- Detect red flags that are identified;
- Respond appropriately when a red flag is detected; and
- Periodically re-evaluate the identity theft prevention program to reflect new risks and make necessary modifications.

In addition to documenting policies and procedures, your business also must incorporate the compliance program into daily business operations -- much like HIPAA compliance. The program

must be approved by the organization's board of directors (or senior leadership), with designation of a compliance officer. And, because employees play such an important role in preventing and detecting identity theft, your program also must include staff training.

For more information about the Rules or to create an identity theft prevention program appropriate for your business, please contact your Butzel Long attorney.

[1] The Fair and Accurate Credit Transaction Act (FACTA) amends the federal Fair Credit Reporting Act. 15 USC 1681m(e).

For previous e-news or to learn more about our law firm and its services, please visit our website at: www.butzel.com

Butzel Long Offices:
Ann Arbor
Bloomfield Hills
Boca Raton
Detroit
Lansing
New York
Palm Beach
Washington D.C.

Alliance Offices:
Beijing
Shanghai
Mexico City
Monterrey

Member:
Lex Mundi