RED FLAGS RULE

The Red Flags Rule is an anti-fraud regulation issued by the Federal Trade Commission (FTC), requiring businesses and organizations subject to the regulation to implement written programs to identify, detect and respond to the warning signs, or "Red Flags," that could indicate identity theft.

Who Does It Apply To: The Rule applies to "Financial Institutions" and "Creditors" with "Covered Accounts".

"Financial Institution": "Financial Institution" means a state or national bank, a state or federal savings and loan association, a mutual savings bank, a state or federal credit union.

"Creditors": "Creditor" means any business or organization who **regularly** extends, renews, or continues credit; any person who regularly arranges for the extension, renewal, or continuation of credit; or any assignee of an original creditor who participates in the decision to extend, renew, or continue credit. Accepting credit cards as a form of payment does not in and of itself make an entity a creditor. "Creditors" may include finance companies, automobile dealers, mortgage brokers, utility companies, health care providers, service professionals such as accountants, telecommunications companies, retailers that issue credit cards or that have payment plans, colleges and others.

"Covered Accounts": "Covered Account" means:

a. An account that a financial institution or creditor offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions, such as a credit card account, mortgage loan, automobile loan, margin account, cell phone account, utility account, checking account, or savings account; and

b. Any other account that the financial institution or creditor offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the financial institution or creditor from identity theft.

What To Do If The Rule Applies: If the Rule applies, the business or organization must develop and implement a written program to identify, detect and respond to the warning signs, or "Red Flags," that could indicate identity theft. The program must be appropriate to the size of the business or organization.

Each written program also must include reasonable policies and procedures on these four required elements:

1. Identifying Red Flags. Identify Red Flags applicable to covered accounts and incorporate those flags into the program. In identifying flags, four risk factors should be considered: the types of covered accounts offered or maintained, the methods used to open a covered account; how access is provided to a covered account; and previous experience with identity theft. The FTC has identified 26 examples of Red Flags that it has organized into five categories:

- alerts, notifications or warnings from a consumer reporting agency, such as a fraud alert included in a consumer report or a notice of credit freeze;
- presentation of suspicious documents, such as a forged driver's license or health insurance card, or if the information on the identification card is inconsistent with information provided by the person presenting the identification or with accessible information;
- presentation of suspicious personal identifying information, such as a Social Security number or insurance number that is the same as one submitted by other persons opening accounts, or the person opening an account fails to provide all of the required personal identifying information (e.g., the person provides a health insurance number but no card);
- suspicious activity on an account, such as unusual billing patterns, or notification that account statements are not being received; and
- notice from the customer, law enforcement or others about possible identity theft.

2. Detecting Red Flags. Policies and procedures implemented through the program should address detecting Red Flags both in connection with opening new covered accounts and maintaining existing covered accounts. When verifying the identity of the person who is opening a new account, reasonable procedures may include getting a name, address, and identification number and, for in-person verification, checking a driver's license or passport. To detect Red Flags for existing accounts, your program may include reasonable procedures to authenticate customers (for example, passwords and PIN numbers), monitor transactions, and verify the validity of change-of-address requests.

3. Responding to Red Flags. Response policies and procedures when a Red Flag is detected are critical. The Rule requires an "appropriate" response to prevent and mitigate identity theft. An appropriate response can include one or more of the following: monitoring a covered account for evidence of identity theft; contacting the customer; changing passwords or security codes; closing an existing account; reopening an account with a new account number; not opening a new account; or notifying law enforcement.

4. Periodic Updating. Effective programs must include procedures for periodic updates to ensure that the program keeps current with identity theft risks, technology changes or tactics of identity thieves.

In addition to the four core elements, the Rule requires that the program be approved by either the company's board of directors, an appropriate committee of the board of directors or senior management if there is no board. The board, committee or a designated member of senior management of the company must be involved in the oversight, development, implementation and administration of the program. Staff must be trained, as necessary, to implement the program.

The FTC has delayed enforcement of the Rule until June 1, 2010.

For more information of the Red Flags Rule, go to http://www.ftc.gov/redflagsrule

Michael J. Weiner, Esq.
GLASER & WEINER, LLP
175 East Shore Road, Suite 300
Great Neck, NY 11023
516.304.5858
mweiner@glaserweiner.com
www.glaserweiner.com

Michael Weiner provides general business and transactional representation to public and private companies on Long Island. My practice includes transactional representation of clients in purchases and sales of businesses, asset based financings and other commercial loan transactions, intellectual property licensing, venture capital financings and securities offerings. I also provide day-to-day business counsel to my clients on a wide range of matters and negotiate various agreements (shareholder, distribution/supply, web development, service, employment/consulting, licensing and technology transfer, LLC operating and confidentiality) on their behalf.