

Celebrating 25 years of dedicated service to clients in the communications industries.

To: All Clients

October 15, 2008

**NEW FTC "RED FLAG" REGULATIONS REQUIRE
BUSINESSES EXTENDING CREDIT TO ADOPT AND IMPLEMENT
IDENTITY THEFT PREVENTION PROGRAMS
BY NOVEMBER 1, 2008**

The Federal Trade Commission ("FTC") has issued new regulations requiring certain financial institutions and other creditors to adopt and implement a written identity theft prevention program. The program adopted must be designed to alert the entity to the existence of "red flags" indicating a potential risk of identity theft in order to prevent such occurrence, and to mitigate damages from identity theft should it occur. Programs must be formally adopted by an entity's board of directors, a committee of the board, or designated personnel at the senior management level if the entity does not have a board of directors, and must be implemented **by November 1, 2008**.

Any party that regularly extends, renews, or continues credit, including deferring payment in connection with the purchase of goods or services, is by definition a creditor subject to the "red flag" regulations. Entities subject to the new regulations include those offering or maintaining accounts (primarily for personal, family, or household purposes) that involve multiple payments or transactions, such as credit card accounts, mortgage loans, checking accounts, or other accounts for which there is a reasonably foreseeable risk of identity theft.

While the "red flag" rules are primarily intended to protect individual consumers, under certain circumstances an entity may also be required to protect its business customers if there is the risk for identity theft. Thus, broadcasters are subject to, and must comply with the new "red flag" rules when they sell advertising to small businesses or sole proprietorships and defer payment until after the advertising runs, and communications

businesses are deemed to be creditors subject to the new rules if they sell goods and services to consumers or certain business customers and collect payment in arrears or pursuant to installment plans.

"Red Flag" Rule Requirements

An entity subject to the "red flag" rules must do the following:

1. Periodically Identify Covered Accounts.

An entity must periodically assess whether it offers or maintains accounts subject to the "red flag" rules, and evaluate:

- the methods used to open its accounts;
- the methods used to access its accounts; and
- prior experiences with identity theft.

2. Establish an Identity Theft Prevention Program.

An entity must adopt and implement an identity theft prevention program, which must include:

- a method to identify which "red flags" are indicators of a possible risk of identity theft for the covered accounts;
- a method to detect "red flags" when they arise;
- a method to respond appropriately to any "red flags" detected in order to prevent identity theft and mitigate damages that result from identity theft; and

- a method by which the identity theft protection program is updated periodically to reflect changes in risk to customers and to the protection of the creditor from identity theft.

3. Administration of a “Red Flag” Program.

Upon adoption of the identity theft prevention program, the board of directors or a designated employee at the level of senior management must be responsible for implementation and oversight of the program, and will be the primary person designated to review reports prepared by staff regarding compliance, and to approve material changes to the program as necessary to identify theft risks.

- *Reports:* Designated staff should report, at least annually, to the board of directors with respect to compliance with the FTC’s “red flag” rules. The report should include an assessment of the effectiveness of the identity theft prevention program in addressing the risk of identity theft in connection with the opening of new covered accounts and of existing accounts; service provider arrangements (see below); significant incidents involving identity theft that occurred during the reporting period, and management’s response; and recommendations for material changes to the program.
- *Service Provider Arrangements:* If a business engages a third-party service provider to service covered accounts, then steps must be taken to ensure that the activity of the service provider is conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft.

Address Discrepancies

In addition to the identity theft rules discussed

above, the FTC has also adopted “address discrepancy” rules targeted to users of consumer credit reports. If an entity utilizes consumer reports in connection with the extension of credit to a current or potential customer, as part of a background check for employment purposes or otherwise, the entity must establish policies and procedures for dealing with instances where the consumer reporting agency identifies a substantial discrepancy between the address provided by the customer in its credit or employment application and the address that the consumer reporting agency has on file for that customer. Such a discrepancy is a “red flag” alert to possible identity theft.

Penalties

The FTC may impose civil monetary penalties of up to \$2,500 per violation for knowing violations of the “red flag” rules or the “address discrepancy” rule that constitute a pattern or practice. The FTC may also use its adjudicatory authority to issue cease and desist orders and other enforcement actions. States’ Attorneys General can also seek civil damages of up to \$1,000 per violation plus attorney fees for each willful or negligent violation. Although there is no private right of action for noncompliance with the “red flag” rule, victims of identity theft may also bring claims under other theories of liability, including negligence. We therefore strongly recommend that you become familiar with the “red flag” and “address discrepancy” rules, and that you strictly comply with these requirements.

If you are uncertain about whether the “red flag” rules apply to you, if you would like assistance in developing your “red flag” program, or if you have any other questions about these regulations, please contact S. Jenell Trigg (strigg@lsl-law.com), Katrina Gleber (kgleber@lsl-law.com), or Keith Apple (kapple@lsl-law.com) in our office.

Leventhal Senter & Lerman PLLC