

Questions?

If you have any questions about this update, please contact:



Catherine F. Intravia, Partner
cintravia@goodwin.com
(860) 251-5805

The Red Flag Program Clarification Act of 2010: Do The Red Flag Rules Apply To You?

The so-called “red flag rules” (the “Red Flag Rules” or “Rules”), promulgated by the Federal Trade Commission (“FTC”), implemented Section 114 and 315 of the Fair and Accurate Credit Transactions Act (“FACTA”) and had a final compliance deadline of December 31, 2010. Recently, President Obama signed into law the Red Flag Program Clarification Act of 2010 (the “Clarification Act”) to limit the circumstances in which ‘creditors’ will be subject to the Red Flag Rules.

What are the Red Flag Rules all about?

The Red Flag Rules require the creation and implementation of a written Identity Theft Prevention Program. The Program must identify those events or indicators (“red flags”) applicable to your business which would alert you to attempts by unauthorized persons to obtain goods or services as the fruit of an identity theft. (See below for examples of typical red flags). The Program must describe an appropriate response to prevent and mitigate the identity theft, provide for regular updates to the Program to address changing circumstances, and be approved by the Board of Directors (or other governing body) of the applicable business.

Do the Red Flag Rules apply to you?

From the onset, the Red Flag Rules applied to financial institutions and ‘creditors.’ As originally

drafted, ‘creditor’ included anyone who “regularly extends, renews, or continues credit” or “who regularly arranges for the extension, renewal, or continuation of credit.” The Clarification Act narrows this definition by excluding anyone who advances funds on behalf of a person for expenses incidental to a service provided by the creditor to that person (eg. a doctor who pays for a test for a patient and the patient reimburses him later when the bill is paid or an attorney who pays a fee for a client and the client pays when she pays the bill. Specifically, the Clarification Act states that the Red Flag Rules apply to a creditor that regularly and in the ordinary course of business: (i) obtains or uses consumer reports, directly or indirectly, in connection with a credit transaction; (ii) furnishes information to consumer reporting agencies in connection with a credit transaction; or (iii) advances funds to or on behalf of a person, based on an obligation of the person to repay the funds or repayable from specific property pledged by or on behalf of the person; however, a creditor that falls under (iii) is excluded from the requirements of the Red Flags Rule if the creditor advances funds for expenses incidental to a service provided by the creditor to the person.

If you must comply with the Red Flag Rules, what do you need to do?

As noted above, the Red Flag Rules require the



creation and implementation of a written Identity Theft Prevention Program. The program must be approved and managed by the Board of Directors or other senior employees of the business and must include appropriate staff training and oversight of third party service providers. Under the Rules, the business has the flexibility to determine what “red flags” are applicable to the specific business and to develop applicable response procedures. To assist in determining what “red flags” might be applicable to a business, the FTC has developed 26 examples of “red flags” in five general categories. For example, under the consumer reporting agency notification category, examples of “red flags” include a fraud or active duty alert or notice of credit freeze on the report and a pattern of activity inconsistent with the history and usual pattern of the consumer. Under the suspicious documents category, examples of “red flags” include identification documents that

appear altered or forged, photos or descriptions of the consumer that are not consistent with the consumer presenting the identification documents, information presented that is inconsistent with readily available information on file, and an application that appears altered, forged, or reassembled. Examples of “red flags” under the suspicious personally identifying information category include a suspicious address and information from the consumer that is inconsistent.

Questions or Assistance:

If you have any questions about the application of the Red Flag Rules to your business or the types of procedures that would comply, please feel free to contact Catherine Intravia at 860.251.5805.

This communication is being circulated to Shipman & Goodwin LLP clients and friends. The contents are intended for informational purposes only and are not intended and should not be construed as legal advice. This may be deemed advertising under certain state laws. © 2011 Shipman & Goodwin LLP.

One Constitution Plaza
Hartford, CT 06103-1919
860-251-5000

300 Atlantic Street
Stamford, CT 06901-3522
203-324-8100

1133 Connecticut Avenue NW
Washington, DC 20036-4305
202-469-7750

289 Greenwich Avenue
Greenwich, CT 06830-6595
203-869-5600

12 Porter Street
Lakeville, CT 06039-1809
860-435-2539

www.shipmangoodwin.com