

Consumer Protection Client Service Group

To: Our Clients and Friends

November 2, 2009

THE FTC POSTPONES THE DEADLINE FOR RED FLAGS RULE COMPLIANCE AGAIN TO JUNE 1, 2010

In a last minute announcement, the Federal Trade Commission (“FTC”) has indicated that it will delay the compliance date for the “Red Flags Rule” yet again. Affected businesses now have until **June 1, 2010** to develop and implement a plan as required under the Red Flags Rule. Given that these deadline postponements have come immediately before the scheduled compliance dates, many businesses have already started implementing their plans, though businesses that have not done so have won a brief reprieve.

THE RED FLAGS RULE

Pursuant to the Fair and Accurate Credit Transactions Act (“FACTA”), businesses that are considered “financial institutions,” or “creditors” must create a written program to detect, prevent, and mitigate identity theft. This applies not only to banks, savings and loans, and credit unions, but also to finance companies, automobile dealers, utilities, telecommunications companies, and other businesses that defer payment for goods or services. The compliance deadline was originally scheduled for November 1, 2008, but it has now been extended three times, including this last postponement.

DEVELOPING A RED FLAGS RULE PLAN

The Red Flags Rule calls for businesses to design a written program that is approved by the business’ board of directors. It must then be administered by the board or a management-level employee designated by the board. Furthermore, the business must prepare a report, at least once a year, discussing the effectiveness of the business’ Red Flags program, how their relationships with service providers fits into the Red Flags Program, significant incidents involving identity theft during the year, how the business responded to those incidents, and how the Red Flags Program might be improved. A business is also responsible for ensuring its providers and third-party contractors are in compliance, especially if that contractor is in a “better position” to identify red flags.

As we reported in our [May 1, 2009 Bulletin](#), the Red Flags Rule plan itself should:

1. IDENTIFY What May Constitute a “Red Flag.”

Written programs should identify what events constitute “red flags,” or, put differently, what events indicate possible identity theft. Red flags should include reports from customers or consumer reporting agencies of suspicious activity, and situations in which a business receives suspicious documents, or observes unusual account activity.

2. DETECT Red Flags as they Arise.

Written programs should discuss how the business will detect red flags during their normal operations. This includes discussion of how red flags can be detected when new accounts are opened, or how red flags can be detected when transactions are made involving existing accounts.

3. RESPOND to Red Flags that Have Been Detected.

Written programs should discuss what the business will do in the event that a Red Flag is detected. When evaluating responses, the plan should discuss factors that might indicate that there is a particularly high risk of identity theft. For instance, if a business detects a data security breach in which customers’ records have been accessed, the program might indicate that there is a particularly high risk of identity theft which necessitates increased monitoring of affected accounts for suspicious activity, contacting customers, changing passwords, and contacting law enforcement.

4. UPDATE the Written Program Periodically.

Written programs should be updated often to reflect a business’s understanding of new risks, and new methods for detecting, and preventing, identity theft.

The FTC has made clear, though, the Red Flags Rule does not provide rigid requirements on what constitutes a proper plan. Instead, each program should be tailored to the particular business’ environment. Nonetheless, the FTC has prepared guidelines that may be used by low-risk entities (these materials are available at www.ftc.gov/redflagrule).

ADDITIONAL GUIDANCE ON ENTITIES THAT MUST COMPLY

The FTC has published an FAQ section on its [Red Flags Rule website](#) that includes guidance for specific industries and account types. In addition to the FTC’s guidance, the U.S. District Court for the District of Columbia issued an opinion on October 30, 2009 preventing the FTC from applying the Red Flags Rule to attorneys.

Businesses should be aware that the FTC may provide additional guidance by updating its website, and more courts may rule on the applicability of the Red Flags Rule to particular industries. Companies should also consider whether voluntary implementation before the compliance deadline may be a smart decision. For additional information concerning the Red Flags Rule, or how to design, implement, or oversee your Red Flags Program feel free to contact [David Zetony](#) in Washington D.C. at 202-508-6030, [Roy Hadley](#) in Atlanta, GA at 404-572-4510, or [Toby Butler](#) in Atlanta, GA at 404-572-5907.