BRYAN CAVE
A Broader Perspective

Bulletin

Consumer Protection Client Service Group

To: Our Clients and Friends May 1, 2009

Deadline For Companies to Create "Red Flags" Identity Theft Prevention Program Extended from May 1, 2009 to August 1, 2009.

On April 30, 2009 the Federal Trade Commission ("FTC") announced that it will delay enforcement of the new "Red Flags Rule" until August 1, 2009 to give businesses more time to develop and implement written identity theft prevention programs.

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 to finance companies, automobile dealers, utilities, telecommunications companies, and other businesses that defer payment for goods or services. Although the FTC originally indicated that businesses had to put their new programs in place by November 1, 2008, the compliance deadline was originally extended to May 1, 2009. The extension has now been increased to August 1, 2009.

Although the Red Flags Rule requires businesses to design a written program, and for that program to be approved by a business's board of directors, it does not provide rigid requirements on what ***must*** be included in the program. Instead, the Rule stresses that each program should be tailored to a particular business's environment. Nonetheless, the FTC has indicated that they will provide a template that may be used by low-risk entities, and that each program, whether for a low-risk or high-risk entity ***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.

Each Red Flags Program must be overseen by the Board of Directors, or by a member of senior management. Furthermore, the business must prepare a report, at least once a year, discussing the effectiveness of the business's 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.

For additional information concerning the Red Flags Rule, or how to design, implement, or oversee your Red Flags Program feel free to contact Dana Rosenfeld in Washington D.C., at 202-508-6032, or David Zetoony in Washington D.C., at 202-508-6030.