

Mailing Address  
P.O. Box 6133  
Williamsburg VA 23188



Office Location  
325 McLaws Cr. Suite 2  
Williamsburg VA 23185

Courtesy of:  
Peter Mellette, Esq.  
peter@melletpc.com

## Client Advisory

### FTC Red Flag Rules: Enforcement of Mandated Identity Theft Programs Delayed Until August 1, 2009

**FTC Announces Delay.** On April 30, 2009, the Federal Trade Commission (“FTC”) delayed enforcement of the new “Red Flag Rule” until August 1, 2009 to provide covered entities (including most doctors and other providers as well as creditors and financial institutions) more time to develop and implement written identity theft prevention programs mandated by the Fair and Accurate Credit Transaction Act of 2003.

**Health Care Providers.** The FTC extended the Red Flag Rule to most health care providers in a February 4, 2009 letter to the American Medical Association. The FTC explained that “[i]f a service provider (such as a hospital, doctor, lawyer, or merchant) allows the client or customer to defer the payment of a bill, this deferral of a debt is credit for purposes of the regulation, even though there is no finance charge and no agreement for payment in installments.” In addition, the rules apply to non-profit institutions.

According to the FTC, compliance with both the Red Flags Rule and the Health Insurance Portability and Accountability Act (“HIPAA”) is necessary to implement a comprehensive approach to combat medical identity theft. Unlike HIPAA, which primarily addresses medical information, the Red Flag Rule protects financial information. Nevertheless, the rules go beyond HIPAA, requiring physicians and providers take action should patient information fall into the wrong hands.

**Identity Theft Programs.** The Red Flag Rule requires all covered entities, including health care providers to develop and implement a written Identity Theft Program (the “Program”) that identifies appropriate warning signs or “red flags” and detects patterns and practices that may indicate that an account holder has engaged in or been the victim of identity theft. The Program must incorporate detection and response mechanisms to the triggering events and ensure the periodic update of the Program. Proper implementation requires participation of company officers or directors in developing and supervising the Program, coupled with adequate staff training.

**Civil Penalties.** Serious administrative and civil penalties may result from noncompliance with the Red Flag Rule. The FTC has authority to enforce compliance with administrative penalties or up to \$2,500 in fines per violation. The State Attorney General can recover up to \$1,000 per willful or negligent violation along with attorney’s fees. Finally, consumers may recover in a negligence action the actual amount of the injury and attorney’s fees.

*Courtesy of:  
Peter Mellette, Esq.  
peter@mellettepc.com*

Fortunately, physicians and health care providers already have HIPAA policies in place that provide a foundation upon which to build a red flag compliance program. Nevertheless, each program should be tailored to a physician's or health care practice based on risk level. Qualified legal counsel can provide assistance with creating, documenting, and administering your program.

Please let Mellette PC know if you have any questions or if we can assist you further in drafting your red flag compliance program.