

IDENTITY THEFT PREVENTION PROGRAM DEADLINE POSTPONED; OVERVIEW OF PROGRAM REQUIREMENTS

The Federal Trade Commission ("FTC") announced on October 22 that it is suspending enforcement of a significant part of its Red Flag Rules (the "Rules") until May 1, 2009. The Rules are intended to combat widespread identity theft in many sectors of the economy, including health care. Health care providers are just starting to address or implement these new mandates, and this six-month delay may be a welcome reprieve for many organizations struggling to achieve full compliance.

However, this delay only affects the implementation of the Identity theft prevention program (Program) mandated by the Rules. The postponement does not apply to the other regulations promulgated with the Rules, specifically those which address the duties of users of consumer reports regarding "address discrepancies". (See E-Flash "Health Care Providers And The Red Flag Rules: Time Is Running Out", 08/21/08.)

What does the Program require? The most important requirement is development and implementation of an identity prevention program. The FTC's suspension of enforcement of this requirement for six months is a great opportunity for organizations to refine or even begin a careful process to develop and implement their identity theft prevention program. **The FTC does not advocate a "one size fits all" approach for the process of development and implementation of such a program; instead, please keep in mind that the program may and should be customized to the size, nature, and other specific characteristics of your organization.**

We suggest that the covered entities should take the following steps:

- Assess whether your organization is a "creditor" within the meaning of the Rules and if so, does it possess "covered accounts";
- Assess current practices aimed at preventing identity theft. You can utilize the existing privacy or identity theft prevention programs or policies, including policies and processes regarding background checks, system access audits under HIPAA, and other privacy policies;
- Secure buy-in, participation and sponsorship from the senior management and the board of your organization. The Board of your organization must approve the Program; and
- Secure participation of all relevant parties within your organization in developing and implementing the Program, including management, legal, accounting, information technology, compliance and/or audit department representatives. This should also include appropriate personnel to ensure successful training of all relevant staff.

The Program must be designed to "detect, prevent, and mitigate identity theft" in connection with the covered accounts. While developing the Program, keep in mind that it must provide for:

- Policies and procedures for identifying, detecting and responding to Red Flags (e.g., notifications from credit reporting agencies, alerts initiated by customers or patients, inappropriate or suspicious use of customer's accounts). Also, the Program needs to be an evolving document, enabling modifications or updates to the Program based on newly identified risks or other Red Flags;
- Board level approval and senior management oversight. The Board must not only approve the Program's implementation, but also be informed of the Program's effectiveness annual reports to the Board. Such annual reports should assess the program's effectiveness, cite all significant incidents involving identity theft and management's responses thereto, and recommend any changes to the Program based on such assessment;
- Training of staff to manage the Program. Red Flag rules mandate an effective implementation of the Program. Training is crucial to such effective implementation (including training varied by department or individual role in the Program). Training should also be ongoing to ensure staff's knowledge of the latest Red Flags and other newly discovered risks; and
- Oversight of service provider arrangements (e.g., outsourcers, data or payment processors, and business associates). Service provider arrangements should also be included in management's annual report to the Board.

The FTC requires that each covered entity's Program must be formulated with consideration of detailed Guidelines that add details to the above requirements. Such Guidelines, along with a sample list of Red Flags, may be found in the Federal Register, Vol. 72, No. 217, Friday November 7, 2007 ([Appendix A to Part 681 - 681- Interagency Guidelines on Identity Theft Detection, Prevention, and Mitigation](#)).

Is your organization a "creditor" with "covered accounts?" According to the FTC, many industries and entities were confused regarding application of the Rules to such entities. In particular, such organizations questioned not only being subject to the Rules as "creditors," but also the FTC's jurisdiction over their affairs in the first place. Many organizations informed the FTC that they would not have sufficient time to implement proper identity theft prevention policies by the original deadline. Thus, the FTC concluded that enforcement of the Rules as of the November 1, 2008 compliance date "would be neither equitable for the covered entities nor beneficial to the public." (See the [FTC Enforcement Policy: Identity Theft Red Flag Rules, 16 CFR 681.2](#).) A "creditor" is generally any entity that regularly extends, renews or continues credit. "Covered accounts" include accounts designed to permit multiple payments or transactions (e.g., credit card accounts, accounts for patients, and even business credit accounts may be covered under this regulation). The FTC provides further guidelines to businesses in its [FTC Business Alert](#) regarding Red Flag Rules.

Please let us know if you have any questions or would like us to assist you in creating or administering an identity theft prevention program. For additional information, please feel free to contact us:

- Steve Fox at sjfox@postschell.com, or 202-661-6940.
- Edward F. Shay at eshay@postschell.com, or 215-587-1151.
- Vadim Schick at vschick@postschell.com, or 202-661-6945.

Disclaimer: this E-Flash does not offer specific legal advice, nor does it create an attorney-client relationship. You should not reach any legal conclusions based on the information contained in this E-Flash without first seeking the advice of counsel.

© Copyright 2008 Post & Schell, P.C. All rights reserved
"POST & SCHELL" and the Post & Schell Logo are registered trademarks of Post & Schell, P.C.
[About Us](#) | [Our Attorneys](#) | [Practice Areas](#) | [Publications](#) | [Offices](#)