



Physicians Dedicated to
Excellence in Dermatology™

New FTC Red Flags Rule Must be Implemented by May 1, 2009

The Federal Trade Commission (FTC) released a new rule in November 2007 to protect consumers from identity theft by requiring financial institutions and creditors with covered accounts to implement a written identity theft prevention program. Under the FTC's guidelines, physicians who regularly bill their patients for services rendered (including copayments and coinsurance) are considered creditors and must comply with the red flags rule. *This rule will be enforced by the FTC beginning May 1, 2009.*

Brief history

Congress passed the Fair and Accurate Credit Transactions Act (FACTA) in 2003 which required the FTC to develop rules and guidelines regarding the detection, prevention, and mitigation of identity theft for financial institutions and creditors as defined by FACTA. The FTC, in turn, created the Red Flags Rule. A "Red Flag" is defined as a pattern, practice, or specific activity that could indicate identity theft¹. In this context, identity theft typically means a patient's use of someone else's information to obtain medical care. This kind of identity theft can cause a variety of harms including false billing, the exhaustion of benefits for the innocent victim, or the potentially life-threatening corruption of a patient's medical records. Thus, the FTC is requiring all creditors who have covered accounts to comply with the Red Flags Rule and develop identity theft prevention programs.

A creditor is someone who.....	<ul style="list-style-type: none"> • Extends, renews, or continues credit. • Arranges for someone else to extend, renew, or continue credit. • Is the assignee of a creditor who is involved in the decision to extend, renew, or continue credit.
A covered account is.....	<ul style="list-style-type: none"> • an account used mostly for personal, family, or household purposes, and that involves multiple payments or transactions • an account for which there is a foreseeable risk of identity theft

Assessing the Red Flags Rule and its Impact on Dermatology

To meet the requirements of the Red Flags Rule, dermatology practices that defer payments must write and implement an identity theft protection plan. The plan must include the following aspects²:

Policy	Example Procedures ²
Identify relevant patterns, practices, and specific forms of activity that are "red flags" signaling possible identity theft and incorporate those red flags into the Program.	<ol style="list-style-type: none"> a) alerts, notifications, or warnings from a consumer reporting agency; b) suspicious documents; c) suspicious personally identifying information; d) suspicious activity relating to a covered account; or e) notices from customers, victims of identity

¹ World Privacy Forum, "Red Flag and Address Discrepancy Requirements: Suggestions for Health Care Providers" by Robert Gellman and Pam Dixon, Available at http://www.worldprivacyforum.org/pdf/WPF_RedFlagReport_09242008fs.pdf.

² Federal Register, Vol. 72, No. 217: Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions Act of 2003 Available at <http://edocket.access.gpo.gov/2007/pdf/07-5453.pdf>.

New FTC Red Flags Rule Must Be Implemented by May 1, 2009

	theft, law enforcement authorities, or other entities about possible identity theft in connection with covered accounts.
Detect red flags that have been incorporated into the Program.	<ul style="list-style-type: none"> a) Obtaining identifying information about, and verifying the identity of, a person opening a covered account. b) Authenticating customers, monitoring transactions, and verifying the validity of change of address requests, in the case of existing covered accounts.
Respond appropriately to any red flags that are detected to prevent and mitigate identity theft.	<ul style="list-style-type: none"> a) Monitoring a covered account for evidence of identity theft. b) Contacting the customer. c) Changing any passwords, security codes, or other security devices that permit access to a covered account. d) Reopening a covered account with a new account number. e) Not opening a new covered account. f) Closing an existing covered account. g) Not attempting to collect on a covered account or not selling a covered account to a debt collector. h) Notifying law enforcement. i) Determining that no response is warranted under the particular circumstances.
Ensure the Program is updated periodically to reflect changes in risks from identity theft.	<ul style="list-style-type: none"> a) The program requires changes in methods of identity theft. b) The program requires changes in methods to detect, prevent, and mitigate identity theft.

How a Dermatology Practice Would Comply With the Ruling

To meet the requirements of the Red Flags Rule, dermatology practices must first develop a written protocol explaining how you will protect your patients from identity theft. The following table gives you guidelines on developing this protocol:

Step 1	Appoint someone within your practice to develop the compliance plan. Insure this “compliance officer” is able to set aside a significant amount of time to develop the plan and enact it in the future.
Step 2	The compliance officer should determine if the practice meets the criteria of the rule. They should first determine if the practice meets the definition of a creditor and if so whether they deal with covered accounts.
Step 3	If the practice is found to be a creditor and deal with covered accounts, the compliance officer should perform an analysis and risk assessment of the practice’s current policies and procedures for fraud transactions. Once the compliance officer has determined what transactions involve the risk of identity theft, he/she should develop policies and procedures for each of those transactions. Each transaction should include a policy explaining how the practice will identify a red flag, the means of detecting the red flag, and a procedure detailing how staff will respond to that red flag. For example, is the identification of new patients being confirmed by checking a photo ID? Does the name on the patient’s insurance information match their ID? If you receive notice that a patient or consumer has been the victim of identity theft, what would you do? Has the practice dealt with identity theft before and if so how was it handled? It would be a good idea to consult your internal HIPAA policies and procedures manual as there could be

New FTC Red Flags Rule Must Be Implemented by May 1, 2009

potential overlap with your identity theft compliance plan. Because the rule allows for flexibility in tailoring your program, if your compliance officer reasonably determines that your practice has a low risk of identity theft, developing a program should be simple and straightforward, with only a few red flags needed. For example, where the risk of identity theft is low, your program might focus on how to respond if you are notified by a patient or consumer that the person's identity was misused at your practice.

Step 4 As applicable, consult your board of directors, practice medical director, owner or appropriate committee within your practice to approve the compliance plan.

Step 5 Train staff that come into contact with patients and would be in a position to check their identity or see other signs that indicate the patient doesn't seem to be who she/he claims to be such as having a different blood type from what is indicated in the medical records. Have an in-service session about it or hand out training materials at a staff meeting. The key step to enforcing this plan is adequate training. Ensure that service providers you use for activities that would be covered by your program, such as debt collectors, have an appropriate program or comply with your program.

Step 6 The compliance officer should re-evaluate the plan every year to determine if changes need to be made. If changes are required, staff should be re-trained on those specific changes.

The American Academy of Dermatology, along with the American Medical Association (AMA), and other medical organizations continue to push the FTC to reconsider applying this "red flags" rule to medical practices. The Academy has questioned this rule and has called for it to be reversed so that dermatology practices are exempt. The Academy will continue to address this issue with the AMA so that compliance becomes more manageable and practical and does not represent an additional administrative burden.

Additional Resources

For additional information regarding the FTC's Red Flags Rule, please visit the following websites:

The Academy's fact sheet on the Red Flags Rule:

<http://www.aad.org/pm/doc/FTCRedFlagsRulesFactSheet.pdf>.

Federal Register Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions Act of 2003, <http://edocket.access.gpo.gov/2007/pdf/07-5453.pdf>

The "Red Flags" Rule: What Health Care Providers Need to Know About Complying with New Requirements for Fighting Identity Theft, <http://www.ftc.gov/bcp/edu/pubs/articles/art11.shtm>

Red Flag and Address Discrepancy Requirements: Suggestions for Health Care Providers, http://www.worldprivacyforum.org/pdf/WPF_RedFlagReport_09242008fs.pdf