

RED FLAG RULES FAQ

Deadline extended until August 1, 2009

BACKGROUND

On October 31 2007, a joint committee of the OCC, Federal Reserve Board, FDIC, OTS, NCUA and the Federal Trade Commission passed the final legislation for Section 114 of the Fair and Accurate Credit Transactions Act of 2003 (FACTA), also known as the Identity Theft Red Flags and Notices of Address Discrepancy or “Red Flag Rules.” The rules require that all organizations subject to the legislation must develop and implement a formal, written and revisable “Identity Theft Prevention Program” (Program) to detect, prevent and mitigate identity theft. **The original November 1, 2008 enforcement date for the Rule was previously postponed to May 1, 2009 and is now August 1, 2009.** The FTC’s most recent delay acknowledges the ongoing debate regarding whether Congress wrote the Red Flags provision too broadly and allows time for further consideration. The delay will also allow affected organizations more time to prepare and develop their compliance strategy.

Q What are the Red Flags my program must identify?

A “A pattern, practice, or specific activity that indicates the possible existence of identity theft.”

Q What are the basic Red Flag requirements?

- Identify relevant Red Flags for covered accounts and incorporate them into your Red Flags Program.
- Detect Red Flags that have been incorporated into your Program.
- Respond appropriately to any Red Flags that are detected to prevent and mitigate identity theft.
- Ensure your Program is updated periodically, to reflect changes in risks to customers or to the safety and soundness of the financial institution or creditor.
- Ensure your Program is properly administrated internally by the appropriate authority.
- Ensure that employees are properly trained to identify Red Flags.

Q Who must comply?

A Banks, mortgage lenders, credit unions, US branches and agencies of foreign banks, US commercial lending companies of foreign banks, and certain “creditors” which is defined as “any person or business who arranges for the extension, renewal, or continuation of credit.” This specifically includes healthcare organizations, universities, utility companies, car dealers, telecommunications companies, debt collectors, and any organization that is not paid in full in advance or at the time of a purchase or service.

Q What is a covered account?

- A personal account that involves or is designed to permit multiple payments or transactions such as a credit card account, mortgage loan, automobile loan, margin account, cell phone account, medical bill, utility account, checking account, or savings account

- Any other account for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the financial institution or creditor from identity theft, including financial, operational, compliance, reputation, or litigation risks.

Q My organization already has risk policies and procedures in place. I should be okay....right?

A Not necessarily. The final ruling requires a separate Identity Theft Prevention Program. The Red Flag Rules requirement takes the general concept of an organizational risk plan further and mandates that a formal, written and revisable risk plan be implemented that is scalable to the organization’s size and complexity; as well as the nature and scope of its activities. However, an organization’s Identity Theft Prevention Program can reference other policies and programs already in place at the organization to avoid duplication.

Did you know?

A car dealership, even those who would assign all financing responsibilities to a third party company, is considered a “creditor” under the Red Flag Rules as the dealership is the party who opens the account. The third party financial company is also considered a “creditor” as they are responsible for safeguarding the maintained account.

What are the penalties for non-compliance?

Understand that “compliance” does not mean “perfection.” If there is an issue, covered entities must show that they made a “reasonable effort” to comply with Red Flag regulations. This is why it is important for a Program to be as thorough and well managed as possible. Other than possible sanctions for non-compliance, entities must also be aware of the expense and damage to their brand that can stem from class action lawsuits filed for non-compliance.

How much time is my organization going to have to spend implementing an Identity Theft Prevention Program?

According to the Federal Financial Institutions Examination Council (FFIEC), the total annual burden (using banks as an example) is 41 hours and is broken down as follows:

- 25 hours to develop a Program;
- 4 hours for developing policies and procedures to assess the validity of changes of addresses;
- 4 hours for developing policies and procedures to respond to notices of address discrepancy;
- 4 hours for training; and
- 4 hours to prepare an annual report.

I am not a financial institution. What kind of impact can this legislation have on my business?

The new rules require that affected organizations add layers of detection to their business as each account or request for an address change on a covered account must be carefully examined for discrepancies. It may also compel employees to take on duties (discovery and assistance

with prosecution) not previously required. Furthermore, institutions with high employee turnover may have to bear additional costs of training, as Red Flag detection training is mandatory.

Who is ultimately responsible for Red Flag compliance issues?

The final rules require approval of the initial written Program by a board of directors or an appropriate committee of the board. (For financial institutions and creditors that do not have boards of directors, the term “board of directors” means “a designated employee at the level of senior management.”) Thereafter, at the discretion of the covered entity, the board, a committee, or senior management may update the Program.

Do I have to cover all 26 Red Flag examples offered by the government?

No, there is room for flexibility, but if your Program does not provide adequate coverage, your organization must have a good justification for non-compliance or potentially face significant penalties.

Are there any other precautionary measures I should be taking?

As a best practice, while creating an Identity Theft Prevention Program, affected organizations should also take time to review and update all existing privacy and security policies. In addition, as employee training on the identification of Red Flags is mandated, this is also an appropriate time to train employees on other risk alleviation practices, such as sensitive data handling procedures.

How do I create an effective program?

Create a Red Flag Rules Task Force

Include either the board of directors, a committee of the board, or an appropriate senior management employee to manage the oversight, development, implementation and administration of your Red Flag Rules plan.

Perform a Risk Assessment

Perform a risk assessment to determine what accounts your organization is involved with are considered “covered accounts.”

Develop Policies

Determine which of the Red Flags are relevant for each type of covered account. Review the 26 suggested examples of Red Flags.

Approve Program

Organizations must obtain approval of the initial written program by the board of directors or a committee of the board.

Educate/Train

Educate the Task Force and organization on the rules and their impact to the organization. Employee training is mandated.

These materials are provided for information purposes only. This does not constitute legal advice, and is not guaranteed to be correct, complete or up-to-date.

Kroll's Fraud Solutions
866 419 2052
www.krollfraudsolutions.com
www.kroll.com

MMC Companies