

The Red Flags Rule: Four Steps to Compliance

Barbara K. Letcher
Newhouse, Prophater, Letcher & Moots, LLC
5025 Arlington Centre Boulevard, Suite 400
Columbus, Ohio 43220
(614) 255-5441
bletcher@nplmlaw.com

If your business or organization is a “financial institution” or “creditor” and maintains “covered accounts”, the Federal Trade Commission’s Red Flags Rule requires that your business or organization implement a written Identity Theft Prevention Program which will allow it to detect the warning signs of identity theft, prevent identity theft from occurring, and mitigate any damage that may result.

Compliance with the Red Flags Rule is a four step process that begins with the identification of identity theft warning signs – “red flags” – that may occur in your business. Once those relevant red flags are identified, the second step of the process is the development of procedures to detect those red flags in your day to day operations. In those cases where red flags surface, the third step in the compliance process requires that you respond appropriately to prevent and mitigate the harm done. Finally, your Identity Theft Prevention Program must be kept current and you must educate your staff to recognize the risks and take appropriate action to address them.

Step One: Identifying Red Flags

“Red flags” are suspicious patterns or practices, or specific activities that indicate the possibility of identity theft. The red flags for any particular business will depend upon the nature of the business, the types of accounts which it maintains, and how those accounts are opened and accessed. The experience of your business or others like it may dictate the relevant red flags. The Red Flags Rule identifies five common categories of red flags which should be considered in developing an Identity Theft Prevention Program for your business or organization. These categories provide examples only and other red flags may be relevant to your particular business or industry.

1. Alerts, Notifications and Warnings from a Credit Reporting Agency

- A fraud or active duty alert on a credit report
- A notice of credit freeze in response to a request for a credit report
- A notice of an address discrepancy provided by a credit reporting agency
- A credit report showing a pattern of activity inconsistent with the person’s history such as a significant increase in the number of inquiries or change in the use of credit, particularly on new

accounts; an unusual number of recently established credit relationships; or an account that was closed because of an abuse of account privileges

2. Suspicious Documents

- Identification that appears to have been altered or forged
- The person presenting the identification does not match the physical description or look like the person in the photograph
- Information on the identification is different from the information given to you by the person presenting the identification or is not consistent with other information provided by the person
- Information on the identification is different from other information on file such as a signature card or a recent check
- An application that appears to have been altered or forged or torn up and reassembled

3. Suspicious Personal Identifying Information

- Inconsistent identifying information such as an address that does not match the credit reports, a social security number that has not been issued or is listed on the Social Security Administration's Death Master File
- Inconsistencies in the information the customer has provided such as a date of birth that does not correlate with the number range on the Social Security Administration's issuance tables
- An address, phone number or other personal information that has been used on an account that is known to be fraudulent
- A fictitious address, an address for a mail drop or prison, an invalid phone number or a phone number associated with a pager or answering service
- A social security number that has been used by someone else opening an account
- An address or telephone number that has been used by an unusually larger number of customers or other persons opening accounts
- The person fails to provide all required personal identifying information on the application or in response to notification that the application is incomplete
- The personal identifying information is not consistent with the personal identifying information already on file
- The person is unable to provide authenticating information beyond what is generally available in a wallet or credit report, for example, the person is unable to answer a challenge question

4. Suspicious Account Activity

- There is a notice of change of address followed by a request for new or additional credit cards or a cell phone or additional authorized users
- A new account used in ways associated with fraud such as much of the available credit being used for cash advances or to purchase merchandise that can easily be converted to cash or the customer fails to make the first payment or makes only an initial payment
- An account that is used in a manner inconsistent with past practices, for example, a significant increase in the use of available credit, a major change in buying or spending patterns or electronic fund transfers or a noticeable change in calling patterns on a cell phone account
- An account that has been inactive for a lengthy period of time suddenly becomes active
- Mail sent to the customer is repeatedly returned as undeliverable even though transactions continue to occur on the account
- Notice that the customer is not receiving their account statements in the mail
- Notice of unauthorized charges or transactions on the account

5. Notice From Other Sources

- Notice that an account has been opened fraudulently by a person engaged in identity theft can come from anyone including a customer, a victim of identity theft, or law enforcement authorities

Step Two: Detecting Red Flags

Once the possible red flags have been identified, a procedure must be established to detect those red flags in your day-to-day operations. These procedures may differ depending on whether identity is verified in person or is verified by telephone, mail, or Internet.

For a person opening a new account, a reasonable procedure for verifying that person's identity may include obtaining a name, address, and social security number. If the verification is done in person, the procedure should include checking a current driver's license or other government issued identification card or a passport. The procedure may also include checking the information obtained against other available information such as a credit report, the Social Security Death Master File, or other publically available information. Whether these additional steps are necessary will depend on the circumstances.

For transactions involving existing accounts, the procedure for detecting red flags may include confirming that the person you are dealing with is really your customer. It

may also include monitoring transactions on the account and verifying the validity of any change of address requests. In an environment where there is greater risk, more sophisticated methods of authentication may be required.

Step Three: Preventing and Mitigating Identity Theft

Once a red flag is detected, the Red Flags Rule requires that you respond to the red flag appropriately. What is appropriate in any given situation will depend on the extent of the risk of identity theft in the particular case. In some cases, a procedure that begins with contacting the customer to confirm the activity on the account may be appropriate. In other cases, notifying law enforcement may be appropriate. In yet others, no response may be warranted.

The Guidelines provided in the Red Flags Rule provide additional examples of appropriate responses once a red flag is detected. These include:

- Monitoring an account for identity theft
- Changing passwords or security codes that allow access to the account
- Reopening the account with a new account number
- Not opening a new account or closing an existing account
- Not attempting to collect on the account or not selling the account to a debt collector

Your written Identity Theft Prevention Program must include both a means to identify and detect red flags that suggest the possibility of identity theft as well as an appropriate response given the risk.

Step Four: Updating Your Program

The risk of identity theft is on the rise and the forms it can take are ever changing as identity thieves become increasingly clever at circumventing existing precautions. The Red Flags Rule requires that your Identity Theft Prevention Program be updated periodically to identify new red flags and ways to detect them in your operation. The timing of these updates can be triggered by changes in your business or in the accounts you offer. The program should be reviewed at least annually to ensure that it is kept current with identity theft risks, methods to detect identity theft, and the experience of your business with identity theft.

Your obligations under the Red Flags Rule do not end with designing a compliant written Identity Theft Prevention Program. Compliance requires that the program is administered in accordance with the Guidelines to the Red Flags Rule. Your initial written program must be approved by your organization's board of directors or an appropriate committee of the board or, if your organization does not have a board, by a member of senior management. Responsibility for overseeing the program can rest with the board or delegated to a designated employee at the level of senior management. Oversight responsibilities include assigning specific responsibility for implementing the

program, reviewing staff reports regarding compliance, and approving material changes to the program.

In those cases where your organization relies on service providers, the service providers must adhere to the same standards you are required to follow if you were performing the tasks in house and your responsibilities include monitoring the service providers to insure their compliance with the Red Flags Rule. This can be done by including a provision in your contract with the service provider which requires that the service provider have its own Identity Theft Prevention Program which complies with the Red Flags Rule or by providing the service provider with a copy of your program and requiring that they take appropriate steps to prevent or mitigate identity theft through their own procedures and providing periodic reports to you.

The person responsible for administering the program should report at least annually to the board of directors or a designated senior manager. The report should evaluate the effectiveness of your program, significant instances of identity theft and your response, and recommendations for material changes to your program. The report should also address any arrangements with service providers for compliance with the Red Flags Rule.

Compliance with the Red Flags Rule is mandatory for those financial institutions and creditors with covered accounts. It is critical that you maintain records demonstrating compliance and that those records are updated periodically to reflect the administration of your Identity Theft Prevention Program.