



# Red Flag Regulation

## WHAT IT IS

The Red Flag Regulation implements Sections 114 and 315 of the FACT Act. It finalizes three distinct requirements – two of which are relevant to automotive, RV and marine dealers, namely:

1. Duties of users of consumer reports regarding address discrepancy
2. Duties of financial institutions and creditors regarding the detection, prevention, and mitigation of identity theft

## WHEN IT IS REQUIRED

Effective January 1, 2008. **Mandatory January 1, 2011.**

## WHAT THE REQUIREMENTS ARE

1. **Users of consumer reports are required to furnish the consumer’s address to the consumer reporting agency that provided the address discrepancy notice, if all of the following conditions are met:**

- Reasonable belief that the consumer report belongs to the consumer
- Establishes a continuing relationship with the consumer
- Regularly, and in the ordinary course of business, furnishes information to the CRA from which the notice came from

2. **Establish an Identity Theft Prevention Program**

Each financial institution or creditor that offers or maintains covered accounts must develop and implement an Identity Theft Prevention Program that is designed to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account.

*Note: Covered accounts are accounts that involve or are designed to permit multiple payments or transactions, such as a mortgage loan and automobile loan. Thus, auto dealers, even those who sell their paper to finance companies, are covered because the rule applies to opening of a covered account. Lenders are covered because the rule applies to maintaining of a covered account.*

### Elements of the Program

The Program must include reasonable policies and procedures to do the following:

1. **Identify** relevant Red Flags and incorporate those Red Flags into its Program
2. **Detect** Red Flags that have been incorporated
3. **Respond** appropriately to any Red Flags that are detected
4. **Update** the Program periodically

### DEFINITION OF TERMS FOUND IN THE RED FLAG REGULATIONS

**Account:** A continuing relationship, such as an extension of credit for property or services involving a deferred payment.

**Address Discrepancy:** Notice sent to a user by a consumer reporting agency (CRA) that informs the user of a substantial difference between the Input consumer address and the address found on the agency’s file.

**Covered Account:** 1.) An account that a financial institution or creditor offers or maintains, primarily for personal, family or household purposes, that involves or is designed to permit *multiple payments* or transactions, such as a mortgage loan and automobile loan; *and* 2.) An account maintained for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the business.

**Creditor:** Any person who regularly extends, renews, or continues credit; any person who regularly arranges for the extension, renewal, or continuation of credit; or any assignee of an original creditor who participates in the decision to extend, renew, or continue credit. Creditors include lenders, such as banks, finance companies, automobile dealers, mortgage brokers, utility companies and telecommunications companies.

**Identity Theft:** A fraud committed or attempted using the identifying information of another person without lawful authority.

**Red Flag:** A pattern, practice or specific activity that indicates the possible existence of identity theft.

**Service Provider:** A person that provides a service directly to the financial institution or creditor.



**Administration of the Program**

Financial institutions and creditors must obtain approval of the initial written Program, involve the board of directors or a designated employee, train staff, and exercise appropriate & effective oversight of service provider arrangements

**Guidelines**

Financial institutions and creditors must consider the guidelines in Appendix A (see next section), and include in its Program those guidelines that are appropriate.

**APPENDIX A: GUIDELINES ON THE IDENTITY THEFT PREVENTION PROGRAM**

**1. Identify relevant Red Flags**

*Financial institutions and creditors should consider the following risk factors identifying Red Flags:*

- Types of covered accounts the dealer offers or maintains
- Methods the dealer provides to open its covered accounts
- Methods the dealer provides to access its covered accounts
- Previous experiences in identity theft

*The Program should include relevant Red Flags from the following categories, as appropriate. Examples of Red Flags from each of these categories are provided as Supplement A at the end of this document.*

- Alerts, notifications, or other warnings received from CRAs and service providers, such as fraud detection services
- Suspicious documents and suspicious personal identifying information, such as suspicious address change
- Unusual use of, or other suspicious activity related to, a covered account
- Notice from customers, victims of identity theft, law enforcement authorities or other persons regarding possible identity theft in connection with covered accounts held by the financial institution or creditor

**2. Detect Red Flags included in the Program**

*Detect Red Flags in connection with the opening of covered accounts and existing covered accounts, such as by the following:*

- Obtain identifying information, and verify the identity of a person opening a covered account
- Policies and procedures from existing Customer Identification Program may be used
- Authenticate customers, monitor transactions, and verify the validity of change of address requests, in the case of existing covered accounts

**HOW FIRST ADVANTAGE CREDCO CAN HELP IN RED FLAG RULE COMPLIANCE**

CoreLogic Credco offers a Red Flag Solution that not only helps meet Red Flag Rule compliance, but also protects you and your consumers from identity theft.

Delivered within seconds, our Red Flag Solution helps you see the whole picture – from suspicious patterns of activity and victim statements in the credit report to possible OFAC matches to inconsistencies in identity information.

The Red Flag Solution includes the following:

**BuyerID Index:** Helps you quickly confirm the customer's identity with an easy-to-interpret numeric score.

**OFAC Screening:** Ensures that your business doesn't unknowingly aid in terrorist financing or any other illegal activities.

**Credit Reporting Services:** Single-source access to credit reports from all three national credit bureaus. The report provides FACT Act alerts and address discrepancy notices.

*\*The information contained herein is provided for information purposes only and does not constitute legal advice. Neither CoreLogic Credco, nor its subsidiaries or affiliates, or their respective directors, officers, employees or agents make any claims, promises or guarantees about the accuracy, completeness or adequacy of the information contained herein. Before changing or implementing policies and practices related to Red Flag compliance, you should consult competent legal counsel who is familiar with the applicable regulations.*



**3. Respond appropriately to detected Red Flags events, to prevent identity theft and mitigate its effects**

*The Program's policies and procedures should provide for appropriate responses to Red Flags detected. Appropriate responses may include the following:*

- Monitor a covered account for evidence of identity theft
- Contact the consumer
- Change the passwords, security codes, etc.
- Reopen a covered account with a new account number
- Not open a new covered account
- Close an existing covered account
- Not attempt to collect on a covered account or not sell a covered account to a debt collector
- Notify law enforcement
- Determine that no response is warranted under the particular circumstances

**4. Update the Program periodically, to reflect changes in identity theft risks to consumers and financial institutions or creditors**

*Changes to the Program may be based on the following factors:*

- The experiences of the financial institution or creditor with identity theft
- Changes in methods of identity theft
- Changes in methods to detect, prevent and mitigate identity theft
- Changes in the types of accounts that the financial institution or creditor offers or maintains
- Changes in the business arrangements of the financial institution or creditor, including alliances, joint ventures and service provider arrangements

---

**SUPPLEMENT A TO APPENDIX A: ILLUSTRATIVE EXAMPLES OF RED FLAGS**

Financial institutions and creditors may consider incorporating into its Program Red Flags, whether singly or in combination, from the following illustrative examples in connection with covered accounts.

***Alerts, Notifications or Warnings from a Consumer Reporting Agency***

1. A fraud or active duty alert is included with a consumer report.
2. A consumer reporting agency provides a notice of credit freeze in response to a request for a consumer report.
3. A consumer reporting agency provides a notice of address discrepancy, as defined in § 334.82(b) of this part.
4. A consumer report indicates a pattern of activity that is inconsistent with the history and usual pattern of activity of an applicant or customer, such as:
  - a. A recent and significant increase in the volume of inquiries;
  - b. An unusual number of recently established credit relationships;
  - c. A material change in the use of credit, especially with respect to recently established credit relationships; or
  - d. An account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor.



**Suspicious Documents**

- 5. Documents provided for identification appear to have been altered or forged.
- 6. The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.
- 7. Other information on the identification is not consistent with information provided by the person opening a new covered account or customer presenting the identification.
- 8. Other information on the identification is not consistent with readily accessible information that is on file with the financial institution or creditor, such as a signature card or a recent check.
- 9. An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

**Suspicious Personal Identifying Information**

- 10. Personal identifying information provided is inconsistent when compared against external information sources used by the financial institution or creditor. For example:
  - a. The address does not match any address in the consumer report; or
  - b. The SSN has not been issued, or is listed on the Social Security Administration’s Death Master File.
- 11. Personal identifying information provided by the customer is not consistent with other personal identifying information provided by the customer. For example, there is a lack of correlation between the SSN range and date of birth.
- 12. Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the financial institution or creditor. For example:
  - a. The address on an application is the same as the address provided on a fraudulent application; or
  - b. The phone number on an application is the same as the number provided on a fraudulent application.
- 13. Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the financial institution or creditor. For example:
  - a. The address on an application is fictitious, a mail drop, or prison; or
  - b. The phone number is invalid, or is associated with a pager or answering service.
- 14. The SSN provided is the same as that submitted by other persons opening an account or other customers.
- 15. The address or telephone number provided is the same as or similar to the account number or telephone number submitted by an unusually large number of other persons opening accounts or other customers.
- 16. The person opening the covered account or the customer fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete.
- 17. Personal identifying information provided is not consistent with personal identifying information that is on file with the financial institution or creditor.
- 18. For financial institutions and creditors that use challenge questions, the person opening the covered account or the customer cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.

*\*The information contained herein is provided for information purposes only and does not constitute legal advice. Neither CoreLogic Credco, nor its subsidiaries or affiliates, or their respective directors, officers, employees or agents make any claims, promises or guarantees about the accuracy, completeness or adequacy of the information contained herein. Before changing or implementing policies and practices related to Red Flag compliance, you should consult competent legal counsel who is familiar with the applicable regulations.*



**Unusual Use of, or Suspicious Activity Related to, the Covered Account**

19. Shortly following the notice of a change of address for a covered account, the institution or creditor receives a request for new, additional, or replacement cards or a cell phone, or for the addition of authorized users on the account.
20. A new revolving credit account is used in a manner commonly associated with known patterns of fraud patterns. For example:
  - a. The majority of available credit is used for cash advances or merchandise that is easily convertible to cash (e.g., electronics equipment or jewelry); or
  - b. The customer fails to make the first payment or makes an initial payment but no subsequent payments.
21. A covered account is used in a manner that is not consistent with established patterns of activity on the account. There is, for example
  - a. Nonpayment when there is no history of late or missed payments;
  - b. A material increase in the use of available credit;
  - c. A material change in purchasing or spending patterns;
  - d. A material change in electronic fund transfer patterns in connection with a deposit account; or
  - e. A material change in telephone call patterns in connection with a cellular phone account.
22. A covered account that has been inactive for a reasonably lengthy period of time is used (taking into consideration the type of account, the expected pattern of usage and other relevant factors).
23. Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's covered account.
24. The financial institution or creditor is notified that the customer is not receiving paper account statements.
25. The financial institution or creditor is notified of unauthorized charges or transactions in connection with a customer's covered account.

**Notice from Customers, Victims of Identity Theft, Law Enforcement Authorities, or Other Persons Regarding Possible Identity Theft in Connection with Covered Accounts Held by the Financial Institution or Creditor**

26. The financial institution or creditor is notified by a customer, a victim of identity theft, a law enforcement authority, or any other person that it has opened a fraudulent account for a person engaged in identity theft.

---

**RESOURCES:**

**Federal Trade Commission**

<http://www.ftc.gov/opa/2007/10/redflag.shtm>

<http://www.ftc.gov/os/2007/10/index.shtm#31>