



Identity Theft “Red Flags” Rule

What are the Red Flag Rules?

The Red Flag Rules is part of The Fair and Accurate Credit Transaction Act 2003 (FACTA) which requires the implementation of an Identity Theft “Red Flags” Rule. The purpose of the rule is to combat Identity Theft and secure the handling of a consumers’ personal information.

What is the effective date of the Red Flag Rules?

The original effective date was 11/1/08 and banks were required to have their policies and procedures in place by then. For other industries the FTC (Federal Trade Commission) announced an extension of the policy effective date as 5/1/09.

Who Needs to be Compliant?

The rule applies to federal banks, state and federal loan associations, mutual savings banks, state or federal credit union, finance companies, auto dealerships as well as mortgage companies and mortgage brokers.

What is Needed to be Compliant?

The Red Flag Rule requires that the policy or program be in writing. Each company should structure their policy and procedures to fit the size of their business. The major requirement is to detect and prevent Identity Theft. Each policy or program must:

- Identify Red Flags
- Detect Red Flags
- Respond to Red Flags
- Be approved by upper management
- Be monitored and periodically updated as new Red Flags are detected

The FTC identified the following 26 “sample” Red Flags. The list is not meant to be comprehensive, but to provide guidance in implementing the policy or program.

1. A fraud alert included with a consumer report.
2. Notice of a credit freeze in response to a request for a consumer report.
3. A consumer-reporting agency providing a notice of address discrepancy.
4. Unusual credit activity, such as an increased number of accounts or inquiries.
5. Documents provided for identification appearing altered or forged.
6. Photograph on ID inconsistent with appearance of customer.
7. Information on ID inconsistent with information provided by person opening account.
8. Information on ID, such as signature, inconsistent with information on file at financial institution.
9. Application appearing forged or altered or destroyed and reassembled.



CERTIFIED CREDIT REPORTING
"A Nationwide Credit Reporting Firm"

10. Information on ID not matching any address in the consumer report, Social Security Number has not been issued or appears on the Social Security Administration's Death Master File.
11. Lack of correlation between Social Security Number range and date of birth.
12. Personal identifying information associated with known fraud activity.
13. Suspicious addresses supplied, such as a mail drop or prison, or phone numbers associated with pagers or answering service.
14. Social Security Number provided matching that submitted by another person opening an account or other customers.
15. An address or phone number matching that supplied by a large number of applicants.
16. The person opening the account unable to supply identifying information in response to notification that the application is incomplete.
17. Personal information inconsistent with information already on file at financial institution or creditor.
18. Person opening account or customer unable to correctly answer challenge questions.
19. Shortly after change of address, creditor receiving request for additional users of account.
20. Most of available credit used for cash advances, jewelry or electronics, plus customer fails to make first payment.
21. Drastic change in payment patterns, use of available credit or spending patterns.
22. An account that has been inactive for a lengthy time suddenly exhibiting unusual activity.
23. Mail sent to customer repeatedly returned as undeliverable despite ongoing transactions on active account.
24. Financial institution or creditor notified that customer is not receiving paper account statements.
25. Financial institution or creditor notified of unauthorized charges or transactions on customer's account.
26. Financial institution or creditor notified that I has opened a fraudulent account for a person engaged in identity theft.

What happens if you don't comply?

You may be liable for financial penalties in the event of an identity theft breach.

How can Certified Credit Reporting help you comply?

Certified Credit Reporting already provides the Fraud Alerts on credit reports for address mismatch, SSN not issued, etc.

We can help you further with confirming the identity of a consumer with products such as Social Search and Level One Authentication Services. For a small fee both Social Search and Level One Authentication can be delivered automatically with each credit request or as a stand alone product. For more information, please contact your sales representative or customer service location.