

# THE IDENTITY THEFT 'RED FLAGS' RULE

The FTC announces delay

BY GEORGE H. MARENTIS, J.D.



As many of you are aware, The Fair and Accurate Credit Transactions Act of 2003 (FACTA) established a requirement for the implementation of an Identity Theft “Red Flags” Rule. The purpose of the rule is to minimize incidents of Identity Theft and Fraud related to the handling of customers’ non-public

information.

On October 22nd the FTC announced a six month extension of the Identity Theft “Red Flags” rule. The new enforcement date is now May 1, 2009.

## WHO NEEDS TO BE COMPLIANT - MORTGAGE BROKERS?

The rule applies to federal banks, state and federal loan associations, mutual savings banks, state or federal credit unions, finance companies, auto dealerships, as well as, mortgage companies and mortgage brokers. Based on conversations with my clients, most were not aware that the complex rule affects them. In fact, it seems the brokers who were aware of the Red Flags Rule, were led to believe all they had to do was pay a little extra to the credit reporting agencies to get the fraud protection, and all would be well - that is not true...

Mortgage Brokers are among those specifically required to comply with the Red Flags Rule.

## WHAT IS THE “RED FLAG” RULE? WHAT’S NEEDED TO BE COMPLIANT?

The rule requires that the program be in writing. There isn’t a “one size fits all” prescribed solution. Each entity has the flexibility to structure its own program

based on its interpretation of the applicability of the rules and its business practices. The major requirement must detect, prevent and mitigate Identity Theft.

Each Identity Theft prevention program must:

- Identify “Red Flags”
- Detect “Red Flags”
- Respond to “Red Flags”
- Be approved
- Be periodically updated.

The Federal Trade Commission identified 26 “sample” Red Flags. The list is not meant to be comprehensive, but provides guidance for consideration in implementing the program.

## 26 “RED FLAGS”:

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.



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, a file of information associated with Social Security numbers of those who are deceased.
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 it has opened a fraudulent account for a person engaged in identity theft.

#### RAMIFICATIONS OF NOT BEING COMPLIANT.

If you do not comply, you may be liable for financial penalties in the event of an identity theft breach. In addition, non-compliance may lead to class action suits. Your failure to have the written program "documents" your company's negligence with respect to preventing identity theft!

*George H. Marentis is President/CEO of Compliance Made Simple, LLC, a company that provides licensing services and other compliance related services to the mortgage lending industry nationwide. For more information see [www.compliancemadesimple.org](http://www.compliancemadesimple.org) or call 303.859.8550. Mr. Marentis has a Juris Doctorate and over 15 years of mortgage lending experience ranging from frontline operations, originations to regulatory and legislative compliance. Information provided in this article is not intended to be legal advice and is informational only.*