

Questions and Answers about the Identity Theft Red Flag Requirements

1. Who is covered by the new Identity Theft Regulations?

The Identity Theft Regulations consist of three different sets of requirements, and each set applies to different parties.

The first requirement deals with address discrepancies, and applies to all users of consumer reports.

The second group of requirements deals with identity theft prevention (the so called “red flags”) and applies to all financial institutions (such as a bank or thrift) and to all other creditors, including private mortgage lenders, and people who regularly arranges for credit.

- The third set of requirements applies to companies that issue credit or debit cards.

These questions and answers explain the address discrepancy and identity theft prevention requirements, but do not discuss the rules applicable to credit and debit card issuers.

2. When do the regulations go into effect?

The joint final rules and guidelines are effective January 1, 2008. The mandatory compliance date for this rule is November 1, 2008.

3. Why did the Federal agencies issue these regulations?

Congress passed a law in 2003 (the FACT Act) that requires the Federal Trade Commission, the Federal Reserve Board, the Federal Deposit Insurance Corporation, the Comptroller of the Currency and the Office of Thrift Supervision (the Agencies) to issue joint regulations and guidelines regarding the detection, prevention, and mitigation of identity theft. This law also requires that these agencies identify patterns and practices that are associated with identity theft, so-called “red flags.”

4. Are private mortgage brokers and lenders covered by these new rules?

Mortgage brokers and mortgage lenders that use consumer reports are covered by the regulations regarding address discrepancies. Mortgage brokers and mortgage lenders that provide credit, or arrange for credit to be provided, are also covered by the “red flag” requirements to establish policies and procedures to prevent identity theft.

5. Are real estate agents covered by these new rules?

If a real estate agent uses credit reports as part of his or her business, the real estate agent is required to comply with the address discrepancy provisions. If the real estate agent provides credit as part of his or her business, he or she is covered as a “creditor” and also has to comply with the identity theft “red flag” requirements. However, even if a real estate agent does not actually provide credit, real estate agents may be considered a “creditor” under the regulation if they regularly arrange for credit to be extended. For example, a real estate agent that routinely helps a homebuyer by pulling credit reports, suggesting potential lenders, and assisting in the loan application process could be viewed as a “creditor” and thereby subject to the regulation. As will be discussed in question number 11 below, a real estate agent who is covered only because he or she “arranges” credit is subject to very minimal requirements.

6. I use credit reports in my business. What am I required to do under the new address discrepancy regulation?

Any user of a credit report must develop a procedure designed to enable that person to reasonably determine that the information in the report relates to the customer or other party for whom the report was obtained, when the user obtains notice of an address discrepancy. In other words, if you obtain a credit report to determine the creditworthiness of a customer, and the report alerts you that there is an address discrepancy, you must have a policy and procedure in place to verify that the report relates to your customer and not another individual. In addition, if you have confirmed an accurate address for the customer, you must have a policy and procedure in place to forward that information to the consumer reporting agency.

7. If I receive a notice of an address discrepancy, what is an acceptable policy and procedure?

If you obtain a notice of an address discrepancy as part of a credit report, you must have a procedure to ensure that the credit report relates to your customer, and not another individual. An acceptable policy and procedure in that case could be that you will compare the other data in the credit report with the identification supplied by the customer, so that you can match date of birth, phone number, and employment information with the credit report data. Another policy and procedure would be to ask to the customer to review the report and verify that the information in the report relates to the customer's credit history.

8. What is my obligation after I verify the correct address?

If you are able to verify the correct address for your customer, the regulations require that you communicate this information to the consumer reporting agency that sent you the notice of address discrepancy, but only if you usually furnish information about your customers to that agency.

9. What are the identity theft regulations applicable to all creditors and parties that arrange credit?

As noted previously, another set of requirements apply to financial institutions and all other creditors, including parties that arrange for credit to be provided. These regulations mandate policies and procedures to detect, prevent and mitigate identity theft, primarily through the identification of practices that are "red flags" for criminal behavior.

10. What accounts are covered by these red flags regulations?

The rules apply to "covered accounts." A "covered account" does not refer to the typical "account" that one may have at a bank or with a stock broker. Rather, it is defined to mean any type of continuing relationship that involves multiple payments or transactions, even if there is no formal account document. Covered accounts include mortgage loans, car loans, escrow accounts, credit card accounts, and cell phone account. An arrangement with a business is a "covered account" if there is "reasonably foreseeable" risk of identity theft. Thus, if you have a lending relationship with a small business, you may need to consider that arrangement as a

covered account if there is a risk that the account could be compromised if the customer's identifying information is stolen.

11. I am a real estate agent and I routinely help homebuyers apply for credit. What do I have to do under the red flags regulation?

If you do not actually extend credit, or hold funds for another, subject to multiple disbursements, the fact that you are a "creditor" under the regulation is not burdensome. The only requirement that you have in this situation is to conduct an "assessment" or review of your business activities on a periodic basis to ensure that you have not begun to actually offer loans or to hold funds subject to multiple disbursements. For example, you could review your business practices and products once a year, and so long as you have not begun controlling funds of others that are subject to multiple withdrawals, you have no further obligations under the regulation. As a matter of best practice, you may want to document this review through a memo to your files.

12. I am a mortgage lender and I have covered accounts, what do I have to do?

Every financial institution and creditor that has at least one covered account must develop a written identity theft prevention program. The program must be designed to prevent, detect and mitigate identity theft in connection with the opening or maintenance of a covered account. The program must include policies and procedures to:

- Identify relevant red flags.
- Detect red flags that have been triggered.
- Respond appropriately to prevent or mitigate identity theft.
- Ensure that the program is updated periodically.

13. How do I establish the red flags program?

The program must be established by management, and must be approved by your board of directors or an appropriate committee of the board. If the creditor does not have a board of directors, the program must be approved by a senior manager. The board, a board committee, or a senior level management official also must be involved in the development of the program

and administration of the program. Staff must be trained to implement the program, and to exercise oversight over contractors and service providers.

14. What are examples of red flags that should be included in our program?

The regulations do not mandate any specific red flags. Instead, they list, in a Supplement to the regulation, the various red flags that exist today, or that have been developed by the agencies, and direct creditors to consider these red flags when developing the program. The Supplement divides red flags into 5 categories:

- I. Alerts and Warnings: For example, a fraud alert included in a credit report, a credit freeze notice, a notice of address discrepancy, a credit history that indicates a recent and unusual behavior or pattern of activity (such as a change in the use of credit).
- II. Suspicious Documents: Forged or altered identification documents, inconsistent information among the various documents, photo in the identification does not resemble individual.
- III. Suspicious Personal Information: Personal information that is inconsistent with publicly available information used by the creditor (e.g., the address on the credit report differs from the address on the I.D.), the social security number has not been issued or is listed as a number assigned to a deceased person, the address or phone number is the same as the address or phone number used in prior fraud, phone number is invalid, the phone number is the same as the number used by a number of other applicants, the applicant failed to provide all required information.
- IV. Unusual Use of Account: The pattern of use of the credit is different than normal (e.g., credit is used for cash advances in higher than typical amounts, credit is used to buy jewelry or expensive electronics not typical of the customer, customer makes an initial payment but not subsequent payments, material increase in the use of available credit, change in electronic transfer patterns, mail sent to the customer is returned repeatedly but the account continues to be used).

- V. Notice from Customers or Law Enforcement: The creditor is notified by a customer, victim of identity theft, or law enforcement that it has opened an account for a person engaged in identity theft.

15. Are there other red flags that I should consider?

Yes, in addition to the red flags contained in the Supplement, a creditor should also consider red flags from other sources, including the experience the creditor or its customers have had with identity theft and supervisory guidance.

16. I have a small lending business; do I need to include all of these red flags in my program?

No, the regulation requires that creditors consider these red flags, but each institution makes its own determination of what red flags are appropriate for its business, after taking into consideration the types of account relationships it has, the methods used for opening and accessing accounts, and its previously experiences with identity theft.

17. Do I need to follow the Customer Identification Program Rules established for banks?

The identity theft regulation does not require the use of the CIP procedures, but suggests that a creditor consider adopting these procedures as part of the program's requirement to detect identity theft red flags. Detection of red flags can also be assisted by monitoring transactions or verifying change in address requests.

Banks and other insured depository institutions have to have in place a "customer identification program" or "CIP" to be used when opening a new account. The program requires that the bank obtain such information as name, date of birth, address, and taxpayer identification number. The bank must verify the information through a Government issued photo I.D. or certified articles of incorporation for a company. Alternatively, the bank can verify the information through other sources, such as public data bases and credit reports.

18. What do I need to do if I discover the existence of a red flag?

The regulation requires that the creditor have in place policies and procedures in the event a red flag is discovered. The potential responses include monitoring the account, contacting the

customer, closing the account, and notifying law enforcement. In some cases, no action may be warranted. The policies should correlate the response with the amount of risk posed.

19. How often does the red flags program need to be updated?

The program must be updated periodically, to reflect changes in technology and identity theft techniques. The update should also reflect the experience of the creditor and changes in the creditor's business.

20. Does the red flags regulation mandate specific oversight responsibilities?

Yes. The board of directors, an appropriate board subcommittee, or a senior management official must oversee the program, and must assign specific responsibility for implementation, review reports, and approve changes.

21. Are reports required?

Yes, annual reports are required regarding the effectiveness of the program and compliance with the regulatory requirements. The report must also discuss arrangements with service providers to assure that these providers are complying with the regulation, significant incidents involving identity theft, and management's response.

22. Where can I find the address discrepancy and red flags rules?

The rules were published in the Federal Register on November 9, 2007 (72 Fed. Reg. 63718).

23. Who can I call for more information about the address discrepancy and red flags regulations?

The FTC Bureau of Consumer Protection, Division of Privacy and Identity Protection, can be reached at (202) 326-2252. You may also call Scott Rinn at NAR's office in Washington, DC at (202) 383-7508.