



Special Alert - ID Theft Rule Goes into Effect May 1

Creditors including Retailers and Communities Affected

New federal rules issued by the Federal Trade Commission and bank regulators go into effect May 1 and will cause financial institutions and other creditors to look closely for identity theft. The rules are commonly referred to as the “red flag” rules. Because storage centers are often involved in the loan process for their buyers and community owners act as a form of creditor as a landlord, the consensus with industry attorneys is that the red flag rules apply to storage centers.

Below is a summary of the new rules. An 11 minute briefing is also available to members on the website. Just log in and find the video on the news page.

The red flag rules push financial institutions and creditors to make sure that people are who they say they are -- authenticating identities will be the name of the game. Red flag rules stipulate that financial institutions and creditors establish a written identity theft prevention program to detect, prevent and mitigate identity theft. The broad terminology used in the regulation includes a contract to purchase a home or lease a site.

So, what must you do to comply? Under the final rules, you must have a written program that includes controls to address the identity theft risks identified. The rule is drafted in a flexible manner that allows members to develop and implement different types of programs based upon their size, complexity, and the nature and scope of their activities. The final rules and guidelines do not require the use of any specific technology, systems, processes or methodology.

In order to comply, develop a policy to deal with identity information you receive like addresses and social security numbers. If a person appears to have misleading or false information you need to report that to the credit reporting agency that you use.

What would a policy look like? The federal agencies provided some guidance in the rule:

You must develop and implement reasonable policies and procedures designed to form a *reasonable belief* that a consumer report relates to the consumer about whom the report was requested and to act when the user receives a notice of address discrepancy.

Examples of reasonable policies and procedures include comparing the information in the consumer report provided by the consumer reporting agency with information you already have on the customer.

What is suspicious behavior that you should be concerned about? The rules offer 26 examples of suspicious behavior that financial institutions and creditors can use as red flag guidelines. The presentation of altered documents, a suspicious address change, a fraud alert on a credit report and other unusual account activities are potential red flags. The idea is to prompt you to go into "authentication mode" and determine whether fraudsters are trying to apply for credit in someone else's name or hijack someone else's accounts. The red flag rules stem from the 2003 Fair and Accurate Credit Transactions Act (FACTA).

Compliance is required as of May 1, 2009. There are penalties for non-compliance.

What are your risks? Imagine that you have a new resident prepared to move into your community. While you are screening for tenancy, the dealer and the lender will be doing ID checks. But they are all doing them independently. The dealer completes the sale and the lender completes the loan. Now the customer is ready to move in, right? Not so fast. The customer also needs to clear an ID check with the utility companies. As of May 1, expect that utility companies will require a face-to-face meeting before utility services are activated for that customer. Unless everyone along that chain of commerce is satisfied that the customer is who they say they are, the transaction could come to a halt.



The dealer and manufacturer are at risk because the homebuyer won't move into a home without utilities. The lender is also at risk as is the community owner. The Red Flags rule has multiple parties involved so it is best for every member category to do sufficient checks to protect themselves.

Summary

Each business that acts as a creditor or financial institution has to:

- Identify relevant red flags and incorporate them into a detection program.
- Detect red flags in customer information.
- Respond appropriately to any red flags detected.
- Ensure the program is updated periodically to reflect changes in risks.

So ask yourself – what does our policy need to address given the information we handle on each customer? How will we scan for identities of the customers? Will that include a credit bureau check or other method? What ID info do we normally review?

The policy must address what to do if a discrepancy is detected. The three major credit bureaus all have white papers, webinars and other materials for you to use – take advantage of those resources.

The FACTA rule provides 26 illustrations of what a red flag for ID theft might be. These are examples that might help to develop your specific program.

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.
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 Social Security Number (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.

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.

Responses to Red Flags. Appropriate responses may include the following:

- (a) Monitoring a covered account for evidence of identity theft;
- (b) Contacting the customer;
- (c) Changing any passwords, security codes, or other security devices that permit access to a covered account;
- (d) Reopening a covered account with a new account number;
- (e) Not opening a new covered account;
- (f) Closing an existing covered account;
- (g) Not attempting to collect on a covered account or not selling a covered account to a debt collector;
- (h) Notifying law enforcement; or
- (i) Determining that no response is warranted under the particular circumstances.