

## Update: Red Flags Rules Due Date Nears—Again

By Jay Malmquist

November 2009

**November 2009 update:** The implementation date originally set for Nov. 1, 2008 has been delayed three times to 2009 dates: May 1, Aug. 1, and Nov. 1. At the request of Congress members, the latest implementation date now extends to June 1, 2010.

Are you feeling besieged, battered, and bewildered? No, not from the economic downturn, the bankruptcies, or the overstocked showrooms, but from the red flag identity theft rules' impending implementation date. Originally scheduled for November 1, 2008, then May 1, 2009, the rules now have an enforcement date of August 1, 2009.

In reality, the current FTC (or whatever the new agency will be named) will probably not knock at your door in August. But beware: The rules are mandatory, not optional, and you do need a written program. If identity theft can be traced to your dealership, either through an employee at the dealership stealing identities or if you did not take steps to prevent a buyer's fraud, the investigating agency will ask to see your program. If you do not have one, you will be fined. Fines from the FTC can be as much as \$11,000 per violation.

### Red Flags Rule Defined

Understandably, your dealership may be confused about how this rule applies and what you need to do. The rule is exceptionally broad, covering everything from large financial institutions down to small, family-owned businesses. But the rule can be simplified by stepping back and examining how and why dealerships are included.

The rule is a subpart of legislation called the Fair and Accurate Credit Transaction Act of 2003 (FACTA). The legislation covers all agencies that create rules for financing, including the FTC, which oversees dealerships. The specific "Identity Theft Red Flags and Notices of Address Discrepancies" portion of the legislation was developed in response to recommendations by the President's Identity Theft Task Force—a group formed to reduce the billions of dollars in fraud losses to businesses as a result of identity theft.

Identity theft occurs when a thief uses another person's information to commit a crime. The stolen information is relevant only if it can identify an individual, such as a name with a social security or credit card number. Red flags are patterns, practices, or activities that indicate the possible existence of identity theft. The Red Flags Rule outlines 26 "flags" in five categories that dealers must examine, plus includes a recommendation to evaluate any additional practices in a dealership where identity theft might occur. The five categories include:

- Alerts, notifications, or warnings from a consumer reporting agency
- Suspicious documents
- Suspicious personal identifying information

- Unusual use of, or suspicious activity related to, the 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

### Key Terms

Before the program requirements are discussed, there are two key terms from the rule that dealers must understand to effectively evaluate how the rule applies to them. The first term is "covered accounts." Covered accounts include information that could allow someone to steal a client's identity, including personal identifying information. This definition is going to include almost all dealerships. If you obtain information such as the buyer's name, address, credit card number, and driver's license number, it is a covered account.

The second key term is "creditor." Anyone who arranges for or assists in the arrangement, extension, renewal, or continuation of credit is considered a creditor under the rule. So if you directly or indirectly set up partial payment plans or installment plans for the purchase of vehicles or for services, you are a creditor. If you arrange for clients to obtain credit to pay for services through a financing company, you are a creditor. However, if you accept full cash, check, or credit card payment at the time of service or purchase, you are not necessarily a creditor. The term's definition may eliminate certain departments from the Red Flags Rule—such as the parts or service departments if they receive only payments in full and do not accept installment payments.

### Red Flags Rule Requirements

After determining whether the Red Flags Rule generally applies to your dealership and which departments it applies to, you should understand the program requirements of the rule. These high-level requirements include:

- A written program designed to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account. The program can be tailored to the size, complexity, and nature of your dealership's practices. There is no one-size-fits-all program, but it must be documented.
- Board of Directors (or executive management if a Board does not exist) oversight and approval. Initial review and annual review thereafter for most dealerships should be acceptable.
- A designated individual responsible for the maintenance and operation of the program. This individual will coordinate activities and answer questions from staff about red flags.

- Oversight of service providers by the dealership. A “service provider” is a person who provides a service directly to the dealership in connection with one or more covered accounts. This is a very broad definition. The dealership should ensure that the activity of the service provider is conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft. The easiest way to accomplish this is through contract language, making sure that you ask for proof of service providers’ compliance annually. It should suffice to get a copy of the provider’s own red flag program documentation.
- Protocol for regularly updating the program. If there are no significant business practice changes, then an annual review should be enough. If business practices have significantly changed, such as the addition of a parts and service center or a merger and acquisition with another dealership, then the program needs to be reviewed to see if additional red flags apply.
- A training program for all employees. In the training session, every employee should receive a copy of the red flag program. Outline key components of the program and review common scenarios, as well as actions employees must take should the scenario occur. This training should be added to new hire orientation programs as well.

The bulk of the effort in implementing the program is in the documentation to show that your dealership has identified the relevant red flags, detected the flags during normal operations, and responded to the flags to prevent and mitigate the identity theft. The majority of red flags are for preventing the spread of additional use of stolen identities after the initial theft has taken place. However, you should consider theft by staff or accidental loss as well.

To identify the appropriate red flags and document your effort, a dealer must conduct a risk assessment. The assessment shows which accounts are included, the threats to the dealership, and an analysis of the 26 red flags from the rule and any additional red flags that may be relevant to dealerships. (When assisting dealerships in red flag program creation, Wipfli typically recommends adding 10-15 additional flags to further protect dealerships in areas not covered by the original 26 red flags.) The assessment can simply state which

flags are applicable and which are not, providing some reason why the nonapplicable flags do not apply.

After the dealership has determined which red flags apply, it should create the detection and response protocol. This can be created in a chart, which should show the following for each applicable flag:

1. Where the flag might occur, such as in loan origination;
2. How the flag can be detected, such as through a credit report or inspection of credentials;
3. Responses to the detection of a flag, such as additional identity validation or denial of the loan; and
4. Any notifications, such as contacting the police.

Remember, the most common incidents will involve someone who has already stolen an identity and is using it to attempt to purchase a vehicle. The dealership is assisting to prevent the spread of more loss because of fraud. If a vehicle is fraudulently purchased, the likelihood of getting back the vehicle or money is slim. So while understandably not the current highest priority of the dealer, the due date is fast approaching, and a written program is required.

#### About the Author

Jay Malmquist specializes in information technology and risk management. He offers clients both strategic and tactical advice to appropriately manage risk for the size and vision of their business. Jay advises clients on complex regulations and technical requirements in a manner that simplifies and tailors material for easy understanding. He has created red flag programs for dealerships and speaks to various industry groups on the topic as well. Contact Jay at 952.548.3489, or e-mail him at [jmalmquist@wipfli.com](mailto:jmalmquist@wipfli.com).

#### About Wipfli LLP

With more than 800 associates and 15 offices across the Midwest, Wipfli ranks among the largest accounting and business consulting firms in the nation. Serving businesses and individuals since the firm’s start in 1930, Wipfli has one of the region’s strongest dealership practices, with an extensive list of clients across the Midwest. For more information, visit [www.wipfli.com](http://www.wipfli.com).