A BRIEF OVERVIEW OF THE RED FLAGS RULE

PREPARED AT THE REQUEST OF GEORGE ALBRIGHT, MARION COUNTY TAX COLLECTOR

BY
S. ALLEN MONELLO, D.P.A.

AND

LARRY PETERS
MANAGING MEMBERS

AUTOMOTIVE INDUSTRY CENTER FOR EXCELLENCE, LLC (AICE)

THIS GUIDE IS NOT LEGAL ADVICE

The Red Flags Rule requires motor vehicle dealers to establish a written identity theft program and implement it no later than November 1, 2008. This program must contain policies, procedures and processes that are followed to prevent, detect and mitigate identity theft.

This guide is only a brief overview to introduce you to the Red Flags Rule; it is not comprehensive. It is recommended that you obtain the assistance of qualified counsel or compliance consultants to develop the plan that will meet the requirements of this rule.

Your dealerships must establish and implement a written identity theft prevention program as required by the Federal Trade Commission's Red Flags Rule, which became effective January 1, 2008 with mandatory compliance on November 1, 2008. This Rule is mandated by the Fair and Accurate Credit Transactions Act of 2003 (FACTA), which amended the Fair Credit Reporting Act (FCRA).

Red Flags

The main purpose of this Rule is to prevent, detect and mitigate identity theft. Dealerships must have policies, procedures and processes in place to accomplish this. When you complete deals with customers, you must be reasonably certain that the customers are who they say they are.

The Rule defines "red flag" as "...a pattern, practice, or specific activity that indicates the possible existence of identity theft." The Rule contains 26 examples of "red flags," some of which are less applicable to dealerships. Here are some of the examples contained in Supplement A to Appendix A of the Rule which are more applicable to your dealerships:

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.
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. 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.
9. 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.
10. 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.
11. 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 a prison; or
    b. The phone number is invalid, or is associated with a pager or answering service.
12. The SSN provided is the same as that submitted by other persons opening an account or other customers.

13. The address or telephone number provided is the same as or similar to the address or telephone number submitted by an unusually large number of other persons opening accounts or other customers.
14. 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.
15. Personal identifying information provided is not consistent with personal identifying information that is on file with the financial institution or creditor.
16. 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.
17. 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.

As identity thieves become more sophisticated, new techniques may be used; therefore, this list of examples is subject to change. You must pay attention to the latest deceptive acts and practices used by identity thieves.

Establishment of an Identity Theft Program

The program you establish must be appropriate to the size and complexity of your dealership and the nature and scope of your activities. The FTC suggests your program include the following:

1. **Identifying Relevant Red Flags**
    a. Risk Factors (sales and leases; employees who have access to account information; previous experience with identity theft)
    b. Sources of Red Flags (previous experience with identity theft at your dealership; ongoing training; management direction)
    c. Categories of Red Flags (alerts or notifications from consumer reporting agencies; suspicious documents; notices from law enforcement agencies or victims of identity theft; suspicious behavior)
2. **Detecting Red Flags**
    a. Obtaining identifying information about and verifying the identity of customers. (What forms of ID do you require? Do you require more than one type of ID?)
    b. Authenticating customers, monitoring transactions, and verifying the validity of change of address requests. (Does the address on the credit report match any of the addresses on the credit application?)
3. **Preventing and Mitigating Identity Theft**
    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.
4. **Updating the Program (based on)**
    a. The experiences of the financial institution or creditor with identity theft;
    b. Changes in methods of identity theft (How are you made aware of the most current scams?);
    c. Changes in methods to detect, prevent, and mitigate identity theft (ongoing training and re-evaluation of methods);

d. Changes in the types of accounts that the financial institution or creditor offers or maintains (prime versus subprime); and
e. Changes in the business arrangements of the dealership, including mergers, acquisitions, alliances, joint ventures, and service provider arrangements.

5. **Methods of Administering the Program**
   a. Oversight of the Program (Company's Board of Directors, Senior Manager)
      1. Assigning specific responsibility for the Program's implementation (Chief Compliance Officer, Chief Financial Officer);
      2. Reviewing reports prepared by staff regarding compliance by the dealership (Who within the dealership is monitoring, reviewing and reporting adherence to policies and processes?); and
      3. Approving material changes to the Program as necessary to address changing identity theft risks. (The plan must be reviewed and revised on a regular basis. Methods used to commit identity theft change; therefore, the plan must be kept current.)
   b. Reports – staff of the dealership should report to the board of directors, an appropriate committee of the board, or a designated employee at the level of senior management, at least annually, regarding compliance by the dealership.
   c. Oversight of service provider arrangements (Which of your service providers have access to customer information?).

PROCEDURES, PROCESSES AND PRACTICES YOU MAY WISH TO ADOPT AT YOUR DEALERSHIP

1) Require at least two forms of identification. One should be a government-issued identification card with a photo (driver license, passport, government employee ID card, military ID, professional license, etc.). The others could be a voter ID card, social security card, credit cards, etc.)
2) Train your staff to recognize fraudulent driver licenses. This would include areas such as DL number not corresponding to year of birth, initial and first three letters of Florida license being different for family members with same last name, physical description on DL not matching individual, etc. Staff can be trained in this area through classes provided by regulatory agencies and/or law enforcement.
3) Look for current and frequent inquiries on credit report.
4) Train staff to always ask customers one or more "challenge questions". For example, while looking at the customer's credit report, ask them:
   a. Which states they have they lived in.
   b. Which financial institution holds their mortgage.
   c. Which addresses they have lived at over the past 5, 10, 15 years.
4. Subscribe to a database that provides you with social security number decoding to determine what year and in which state the number was issued. Also whether that number appears on the Social Security Administration's Death Master File.
5. Train staff on the latest identity theft schemes.
6. Direct staff to report unresolved address discrepancies to Program Coordinator.

There are several things that you must remember when developing your plan.

- **It must be written and it must be customized to your dealership.**
- **It must be updated on a regular basis with regard to the latest information available about identity theft schemes and what steps your dealership has taken toward compliance with the Red Flags Rule.**
- **The policies, procedures and processes must be practiced and adhered to.**
- **All appropriate staff must be familiar with the plan and be trained in their relevant areas regarding the implementation of the plan.**

- **If what you did is not documented, it will be difficult to prove!**

What the written plan should include:

- A statement about who was appointed as the Program Coordinator and who that person will report to.
- A list of the Program Coordinator's duties and responsibilities.
- Address management issues such as:
    - which employees will have access to customer information;
    - obtain written acknowledgements from employees stating they understand the policy and will abide by it;
    - obtain written acknowledgements from service providers; and
    - determine which service providers you will contract with to assist with the implementation of this program and clearly state what information is provided
- Establish policies and procedures with regard to:
    - proof of identification required from customers;
    - steps that employees should take to verify customers' identifies;
    - challenge questions that should be asked of customers;
    - who should be notified when discrepancies occur (e.g., Program Coordinator)
    - when should law enforcement be notified and who should do this

Sample Part of an Identity Theft Prevention Program (ITPP) –THIS IS FOR INFORMATION PURPOSES ONLY AND DOES NOT REFLECT THE ENTIRE PLAN THAT IS REQUIRED TO BE DEVELOPED. THIS SMALL SECTION IS ONLY INTENDED TO ILLUSTRATE HOW PARTS OF AN ITPP PLAN MIGHT BE WRITTEN. THIS PARTIAL SAMPLE IS NOT INTENDED TO GIVE LEGAL ADVICE AND MAY NOT FIT YOUR PARTICULAR DEALERSHIP NEEDS OR OPERATIONS. CONSULT WITH LEGAL COUNSEL TO ENSURE YOUR PLAN MEETS ALL THE REQUIREMENTS OF THE RED FLAGS RULE.

Effective Date and Responsible Parties

All affected employees of _____ (name of dealership) must comply with the foregoing policies and procedures contained in this Identity Theft Prevention Program (ITPP) by November 1, 2008.

_____ (name of individual) is appointed as the coordinator (Compliance Officer) of this plan and is responsible for ensuring compliance with this plan and who will report all progress, findings and statuses to _____ (board of directors, owner, CEO, general manager, etc.).

Purpose

It is this dealership's purpose to develop a comprehensive Identity Theft Prevention Program (ITPP) to detect, prevent, and mitigate identity theft in connection with the opening and processing of covered accounts and other covered transactions in compliance with the Fair and Accurate Credit Transactions Act of 2003 (FACT Act) and Red Flags Rule. This ITPP and the policies and procedures herein have been developed as a good faith effort to comply with these laws to reduce the potential or incidence of identity theft.

Responsibilities

The board of directors (owner, CEO, general manager, etc.) has the authority and responsibility to approve this plan and to ensure that it is carried out.

The Compliance Officer (coordinator or other member of senior management) is responsible for:

- overseeing the development, implementation and adherence to this plan
- assigning responsibility to various dealership staff to carry out certain processes and procedures to comply with this plan and to follow the intent of this law
- reviewing progress made to implement this plan and
- conducting regular risk assessments to detect ongoing threats or changes in patterns or methods of identity thieves.

Accounts offered or maintained by dealership

- consumer vehicle installment sale contracts
- consumer vehicle leases
- business vehicle installment sale contracts
- business vehicle leases
- servicing and collecting on covered accounts (buy here, pay here – if applicable)

Relevant Red Flags for this dealership

(List Red Flags identified above and any others your dealership encounters.)

Detecting Red Flags

(List procedures you want followed here such as requiring more than one form of ID, comparing signatures from driver license and application, examining driver license for fraud, becoming aware of address discrepancy between application and credit report, etc.)

Steps to Follow When Red Flags Detected

(For example, if a discrepancy is detected, ask challenge questions such as 1) where were you born; 2) which states have you lived in; 3) how long have you lived at this address; etc.

- Decide when coordinator/Compliance Officer should be notified
- Determine when you would not go forward with the deal.
- Decide when law enforcement should be called.
- Etc.

Oversight of service providers

Coordinator/Compliance Officer to require written assurance from service providers that their policies and procedures are designed to detect, prevent, and mitigate the risk of identity theft. Service providers are to be monitored for compliance.

Training

Develop a plan and training schedule to ensure that all relevant dealership staff will be trained on a regular basis in identity theft detection, prevention and mitigation. Training must include all relevant new-hires and existing personnel.

Reports – Annual and Updates

Coordinator/Compliance Officer will ensure that the Annual Report is written and presented to management and that all reports of activities and progress are updated as needed.