

**DEVELOPING YOUR DEALERSHIP’S WRITTEN PROGRAM  
TO DETECT, PREVENT, AND MITIGATE IDENTITY THEFT  
AS REQUIRED BY THE “THE RED FLAG RULES” AND  
TO RESPOND TO NOTICES OF ADDRESS DISCREPANCIES**

The Interagency Guidelines on Identity Theft Detection, Prevention and Mitigation, commonly referred to as the “Red Flag Rules”, require each financial institution and creditor that offers or maintains one or more covered accounts, as defined in the Rules, to develop and provide for the continued administration of a written Program to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account. The Rules also deal with Notices of Address Discrepancies received from a credit-reporting agency (CRA). The following information is designed to assist you in the formulation and maintenance of a Program for your dealership that satisfies the requirements of the Rules.

I. Your Dealership Program

In designing your Dealership Program, be sure to incorporate, as appropriate, existing dealership policies, procedures, and other arrangements that control reasonably foreseeable risks to customers or to the safety and soundness of your dealership from identity theft.

II. Identifying Relevant Red Flags

(a) Risk Factors. You should consider the following factors in identifying relevant Red Flags for covered accounts, as appropriate:

(1) The types of covered accounts you offer or maintain; in most dealerships this will include, at a minimum, all sale and lease documents that your dealership uses in the purchase/lease of a new or used motor vehicle;

(2) The methods you provide to open covered accounts;

(3) The methods you provide to access your covered accounts; and

(4) Any previous experiences with identity theft.

(b) Sources of Red Flags. You should also incorporate relevant Red Flags from sources such as:

- (1) Incidents of identity theft that you have experienced;
- (2) Methods of identity theft that you have identified that reflect changes in identity theft risks; and
- (3) Applicable supervisory guidance.

(c) Categories of Red Flags. Your Dealership Program should include relevant Red Flags from the following categories, as appropriate. For your convenience, examples of Red Flags from each of these categories are listed in the section entitled “Red Flag Examples”, located at the end of this document.

- (1) Alerts, notifications, or other warnings received from consumer reporting agencies or service providers, such as fraud detection services;
- (2) The presentation of suspicious documents;
- (3) The presentation of suspicious personal identifying information, such as a suspicious address change;
- (4) The unusual use of, or other suspicious activity related to, a covered account; and
- (5) Notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts held by your dealership.

### III. Detecting Red Flags

The Dealership Program’s policies and procedures should address the detection of Red Flags in connection with the opening of covered accounts and existing covered accounts, by means such as:

- (a) Obtaining identifying information about, and verifying the identity of, a person opening a covered account, for example, by using the policies and procedures regarding

identification and verification that are set forth in the Customer Identification Program rules; and

(b) Authenticating customers, monitoring transactions, and verifying the validity of change of address requests, in the case of existing covered accounts.

#### IV. Preventing and Mitigating Identity Theft in Your Dealership

Your Dealership Program's policies and procedures should provide for appropriate responses to the Red Flags you have detected that are commensurate with the degree of risk posed. In determining an appropriate response, you should consider aggravating factors that may heighten the risk of identity theft, such as a data security incident that results in unauthorized access to a customer's account records held by you or a third party, or discover that a customer has provided information related to a covered account held by you to someone fraudulently claiming to represent the financial institution or creditor or to a fraudulent website. 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.

#### V. Updating Your Dealership Program

You should update your Dealership Program (including the Red Flags determined to be relevant) periodically, to reflect changes in risks to customers or to the safety and soundness of your dealership from identity theft, based on factors such as:

- (a) The experiences of your dealership with identity theft;
- (b) Changes in methods of identity theft;
- (c) Changes in methods to detect, prevent, and mitigate identity theft;
- (d) Changes in the types of accounts that your dealership offers or maintains;

and

(e) Changes in the business arrangements of your dealership, including mergers, acquisitions, alliances, joint ventures, and service provider arrangements.

#### VI. Methods for Administering Your Dealership Program

(a) Oversight of Program. Oversight can be by the board of directors, an appropriate committee of the board or a designated dealership employee at the level of senior management, and should include:

- (1) Assigning specific responsibility for your Program's implementation;
- (2) Reviewing reports prepared by staff regarding compliance with the Rules; and
- (3) Approving material changes to your Program as necessary to address

changing identity theft risks.

(b) Reports. (1) In general. Staff of your dealership responsible for development, implementation, and administration of your Program 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, on compliance by your dealership with the Rules.

(2) Contents of report. The report should address material matters related to your Program and evaluate issues such as: the effectiveness of the policies and procedures of your dealership in addressing the risk of identity theft in connection with the opening

of covered accounts and with respect to existing covered accounts; service provider arrangements; significant incidents involving identity theft and management's response; and recommendations for material changes to your Program.

(c) Oversight of dealership service provider arrangements. Whenever you engage a service provider to perform an activity in connection with one or more covered accounts you should take steps to 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. For example, you could require the service provider by contract to have policies and procedures to detect relevant Red Flags that may arise in the performance of the service provider's activities, and either report the Red Flags to you, or to take appropriate steps to prevent or mitigate identity theft.

### **Red Flag Examples**

*The following are examples of Red Flags provided by the FTC that may or may not be appropriate to your Dealership's 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 a 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 a new, additional, or replacement card 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. 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 statement

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.

**© 2008 by the National Independent Automobile Dealers Association and Keith Whann &  
Associates. Permission to use for educational purposes granted to NIADA members only.  
Not for resale.**