IDENTITY THEFT PROTECTION PROGRAM[1]
(Red Flag and Address Discrepancy Program)[2]

This dealership is committed to protecting its customers and itself from identity theft. To this end, it adopts this Program to establish and implement policies and procedures (1) to identify patterns, practices, or specific activities that indicate the possible existence of identity theft ("Red Flags"), (2) to detect and respond to Red Flags, and (3) to prevent and mitigate identity theft in our dealership, all for consumer transactions involving multiple payments and other multiple payment or credit accounts where there is a reasonably foreseeable risk of identity theft to our customers, to other consumers, or to this dealership.

1. The Coordinator of this program who is responsible for development, implementation and maintenance of the Program is:

2. We have done an assessment of our covered accounts. We have determined that the following departments handle covered accounts: a. Sales (new and used) and F&I b. Parts c._____ d. _____

3. We have identified Red Flags based on those suggested in the FTC Red Flags Rule and the FTC Address Discrepancy Rule, and based on those the dealership determines from its own experience, information from others, and the guidance of supervisory government agencies.
4. We have developed procedures for detecting Red Flags (see Detection Checklist).
5. We have developed procedures for responding to Red Flags (see Response Procedures).
6. The Program Coordinator will oversee training of employees in departments with covered accounts in complying with this Program. The Program Coordinator will implement and oversee a process to train new employees of those departments in compliance with this Program and to train the staff in those departments in the event of updates to this Program.
7. In the event this Dealership outsources to a service provider any activity for opening or maintaining covered accounts, or any duty under this Program, we will take steps to ensure that the service provider has reasonable policies and procedures in place to detect, prevent and mitigate the risk of identity theft in performing those functions.
8. The Program Coordinator will ensure that this Program is continuously administered and is reviewed:
   - as necessary based on incidents of identity theft;
   - as necessary if the dealership learns of (a) new methods or techniques of identity theft or (b) new methods or techniques to detect, prevent and mitigate identity theft; and
   - annually in a detailed report to the person or persons responsible for oversight as shown below.

This program was reviewed and adopted by:
☐ The Board; ☐ A Board Committee; or ☐ the Dealer

Date: _____ _____
on behalf of the Board, its Committee or the Dealer

[1] This program addresses the FTC's Red Flag Rule and the FTC's Address Discrepancy Rule
[2] This is a suggested template to help a dealer in preparing an ITPP program. A dealer must prepare its own program based on materials such as this template and other available resources. This document is for information purposes only, and it is designed to be used only following training in its use. It does not constitute legal advice. For legal advice on the FTC Red Flag Program or the FTC Address Discrepancy Program requirements, contact an attorney for the dealership. This document is designed for a motor vehicle dealer that is not involved in buy here/pay here transactions.

© 2008 Charapp & Weiss, LLP

IDENTITY THEFT PROTECTION PROGRAM DETECTION CHECKLIST

The dealership has determined that the following are Red Flags that may indicate possible identity theft. Each employee doing a credit/lease transaction or opening a covered account for a customer shall detect the existence of any of the following Red Flags by:
1) obtaining a signed credit application that includes the customer's name, date of birth, address, and social security number or taxpayer's ID number;
2) obtaining and photocopying the customer's drivers license or other government issued photo ID;
3) carefully inspecting all documents provided by the customer for signs of alteration or forgery and ensuring that the photo ID matches the customer's appearance;
4) obtaining a consumer report, determining whether there is a fraud or active duty alert, a credit freeze notice, a notice of address discrepancy, or any other alerts or notifications, and reviewing whether the history and activity shown and the information provided in the consumer report are consistent with information provided by the customer;
5) being alert to suspicious statements or behavior of the customer; and
6) comparing the information provided by the customer to any information already on file at the dealership.

A. *Alerts, Notifications or Warnings from a Consumer Reporting Agency*

- ☐ A fraud or active duty alert is included with a consumer report.
- ☐ A consumer reporting agency provides a notice of credit freeze in response to a request for a consumer report.
- ☐ A consumer reporting agency provides a notice of address discrepancy.
- ☐ 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 recent and significant increase in the volume of inquiries; an unusual number of recently established credit relationships; a material change in the use of credit, especially with respect to recently established relationships; or an account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor.
- ☐ _____
- ☐ _____

B. *Suspicious Documents*

- ☐ Documents provided for identification appear to have been altered or forged.
- ☐ The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.
- ☐ Other information on the identification is not consistent with information provided by the person opening a new covered account or customer presenting the identification.
- ☐ Other information on the identification is not consistent with readily accessible information that is on file with the dealership, such as information on the dealership's computer database.
- ☐ An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.
- ☐ _____
- ☐ _____

C. *Suspicious Personal Identifying Information*

- ☐ Personal identifying information provided is inconsistent when compared against external information sources used by the dealership. For example: the address does not match any address in the consumer

report; or there is a notice by the consumer reporting agency of a discrepancy on the social security number.

- ☐ Personal identifying information provided is of a type commonly associated with fraudulent activity by internal or third-party sources used by the dealership. For example: the address on an application is fictitious, a mail drop, or a prison; the phone number is invalid, or is associated with a pager or answering service; or the information is the same as that provided by other customers of the dealership.
- ☐ 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.
- ☐ 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.
- ☐ Personal identifying information provided is not consistent with personal identifying information that is on file with the Dealership.
- ☐ _____
- ☐ _____

D. *Unusual Use of, or Suspicious Activity Related to, the Covered Account*

- ☐ _____
- ☐ _____

E. *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.*

- ☐ The dealership has been 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.
- ☐ _____
- ☐ _____

F. *Other "Red Flags" based on the Dealership's own experiences, information from other dealerships, businesses, or associations, or based upon supervisory governmental agency advice or updates.*

- ☐ _____
- ☐ _____
- ☐ _____
- ☐ _____
- ☐ _____

IDENTITY THEFT PROTECTION PROGRAM RESPONSE PROCEDURES

GENERAL RESPONSE TECHNIQUES

In the event of a Red Flag, dealership personnel will respond appropriately to prevent or mitigate identity theft. When a Red Flag is detected:

- Do not proceed with the transaction or open the account until further reasonable procedures are taken to determine the identity of the person with whom the dealership is dealing.
- Request further identification information from the customer, and, if necessary third party sources.
- Fully assess the risk presented by the Red Flag
- Satisfy yourself that there is no reasonable basis to believe that identity theft is involved. If satisfied, no further response is warranted.
- If there is a continuing concern, contact a supervisor, and if possible the Program Coordinator, to further discuss the matter and determine a course of action.
- Do not complete the transaction or open the account unless you and the supervisor (and Program Coordinator, if available) have a reasonable basis to believe identity theft is not involved.

If you complete a transaction or open an account and form a belief that identity theft has occurred consider the following actions:

- Notify the customer
- Notify law enforcement
- Notify any creditor to whom the obligation has been assigned
- Freeze all further activity
- Stop any collection action
- Notify other departments of the dealership in the event the vehicle is returned
- Notify the Program Coordinator

Response in the event of a fraud or active duty alert:

- Take all appropriate steps to confirm the consumer's identity and to confirm that the application for the transaction or to open the account is not the result of identity theft using the General Response Techniques.
- In the event of a notification in the consumer report that the customer must be contacted, contact the consumer only using the telephone number or other means of contact stated in the alert and obtain authorization to proceed with the transaction or open the account.

In the event of a notice of credit freeze, take the following steps:

- Follow the General Response Techniques.
- Do not proceed with the transaction or open the account.
- Proceed once you have received notification that the freeze has been lifted and a credit report has been obtained.

In the event of a notice of address discrepancy on a consumer report:

- Follow the General Response Techniques.
- Do not proceed until you have verified the address and you form a reasonable belief that you are dealing with the consumer whose report was requested.