Livonia Chrysler Jeep Identity Theft Prevention Program

It is Livonia Chrysler Jeep policy to develop, implement, and maintain a comprehensive Identity Theft Prevention Program (ITPP) to detect, prevent, and mitigate identity theft in connection with the opening of all covered accounts or, if there are cases where the Dealership has retained a covered account, in connection with existing covered accounts. For purposes of the Program, and the RED FLAGS RULE discussed below, "identity theft" occurs when a person commits or attempts to commit fraud using identifying information of another person without authority.

This Program is intended to comply with the requirements of the Identity Theft Rules (16C.F.R. part 681), issued by the Federal Trade Commission (FTC) in compliance with Sections 114 (Red Flags Rule) and 315 (Address Discrepancy Rule) of the Fair and Accurate Credit Transactions Act of 2003 (FACT Act), 15 U.S.C. 1681m(e) and 15 U.S.C. 1681c(h).

No part of this Program or related policies and procedures should be interpreted as contravening or superseding any other applicable legal and regulatory requirements. This Program and its related policies and procedures reflect Century Sales Inc.s good faith efforts to comply with applicable law and reduce the potential for identity theft. They do not represent warranties, representations, or contractual obligations in favor of any person or group.

Under this Program, the board of directors of Livonia Chrysler Jeep has the authority and responsibility to:

Approve this ITPP

The Compliance Office, a member of Livonia Chrysler Jeep.s senior management, has been designated to supervise the overall management of the ITPP. The compliance Officer has the authority and responsibility to:

Oversee and manage the development, implementation, and administration of the ITPP.

Assign specific responsibility for the Program's implementation, including but not limited to appointing, supervising, and managing the activities of the Program Coordinator and others having specific responsibility related to the ITPP.

Review reports prepared by staff regarding compliance by Livonia Chrysler Jeep with the Red Flags Rule and this Program.

Approve material changes to the Program as necessary to address changing identity theft risks.

Exercise management control as necessary to ensure that all relevant Dealership operations and employees make compliance with this Program an integral part of regular operations.

The Program Coordinator has been designated to manage and coordinate the ITPP under the supervision and management of the Compliance Office. As deemed necessary by the Compliance Officer, such as at the inception of this Program, the role of Program Coordinator may be undertaken by a team of employees designated by the Compliance Officer.

All affected employees of Livonia Chrysler Jeep must comply with the terms of this policy as instructed by their respective supervisors but no later than November 1, 2008.

Program Development and Assessment

The Red Flags Rule requires Livonia Chrysler Jeep to initially (and periodically thereafter) determine whether it offers or maintains "covered accounts" as defined by the Rule. To do so, we will evaluate each account offered or maintained by Livonia Chrysler Jeep to determine if it is a covered account.

The Risk Assessment for determining whether certain accounts are covered accounts is similar to the Risk Assessment to be used in identifying Red Flags. Therefore, in connection with the periodic identification of covered accounts and identification of relevant Red Flags, we will conduct a Risk Assessment of its accounts and, at a minimum, will take the following factors into consideration:

The types of accounts we offer or maintain

The methods we employ to open accounts

The methods we employ to access accounts

Previous experiences with identity theft

It is Livonia Chrysler Jeep policy to scan every customer's driver's license through The State Of MI Web site before a vehicle is delivered. If any alert is noted, you must notify the Sales Manager and/or Finance Manager and it will be acknowledged immediately to resolve any of the Red Flags posted.

The 25 Red Flags to look for are:

1. Fraud alert on credit report
2. CRA freezes credit – no report when requested.
3. CRA issues notice of address discrepancy
4. Active Duty Alert
5. Credit report indicates odd patterns of use, inquiries, et.
6. Identification documents appear altered
7. Photo does not match person's appearance
8. Information or I.D. is inconsistent with information produced by customer
9. Information is inconsistent with financial institution's information
10. Information is inconsistent with an external information source (SSN is listed on death master file).
11. I.D. information is same as that on a prior fraudulent application
12. SSN is the same as another customer's or SSN has not been issued.
13. Customer refuses to fully complete application
14. Information on application is inconsistent
15. Address on application is a P.O. Box or phone number is a pager or answering service
16. Dealer is notified by a customer, lender, victim of I.D. theft, police, or other person of potential I.D. theft (Ask if they made a police report)
17. Customer wants to sign a credit sale
18. Customer demands off premises delivery and execution of contract or lease
19. Co-buyer in on contract but not present to sign
20. Customer refuses to allow license to be copied or give a thumbprint for a check
21. Customer seeks to buy or lease several vehicles at one time or within a short period of time
22. Customer asks to have contract or lease indicate a different address than on I.D.
23. Customer's trade in is titled in another's name
24. Down payment check is written on someone else's account
25. Incidents involving identity theft experienced by the dealership

Some responses to Red Flags depend on the nature and severity of the Red Flag detected. We will be as flexible and recognize that with reasonable investigation, a red flag can be cleared. With certain red flags, we must take specific action. It is the policy of the dealership to respond appropriately to relevant Red Flags that are detected in a manner intended to prevent or mitigate identity theft, commensurate with the degree of risk posted.

The Program Coordinator shall create and maintain a log of all incidents involving identity theft.

Training

It is the responsibility of the Program Coordinator and Compliance Office to ensure that all relevant dealership personnel receive training, as necessary, to effectively implement the program. The training will include the following:

Distribution of a copy of this Program. Each employee shall sign a written acknowledgment and agree to abide by the program.

Training of all new employees having duties that may involve consumer credit reports or involve the opening of a covered account.

The Training program shall include, at a minimum, basic steps to maintain the security, confidentiality and integrity of customer information, such as:

Locking rooms and file cabinets where paper records are kept

Using password-activated computer software, systems applications or terminals or an automatic log-off function that terminates access after a short period of inactivity.

Changing passwords periodically and maintaining the security of passwords.

Sending electronic information over secure channels only.

Appropriately disposing of paper and electronic records.

Not making available computer screens that contain other customer's non-public information.

Training will occur on a recurring, periodic basis, at least once a year to reflect changes to the program.

All persons who fail to comply with the Dealership's Program shall be subject to disciplinary measures, up to and including termination of employment.