PREPARED AS GUIDANCE FOR NAAA MEMBERS – DO NOT USE WITHOUT CONSULTING LEGAL COUNSEL.

[NAAA MEMBER NAME] IDENTITY THEFT PREVENTION PROGRAM

Program Overview and Purpose:

Protecting the personal identification information of our customers and preventing identity theft have long been priorities for **[NAAA MEMBER NAME]** ("the Company"). The Company has always encouraged the careful use and safeguarding of sensitive customer information collected as a necessary part of its business.

This document furthers those efforts and establishes the Identity Theft Prevention Program (the "Program") of the Company. The purpose of this Program is to formalize policies, practices, and procedures aimed at detecting and combating the potential occurrence of identity theft in the Company's customer accounts. Furthermore, this Program is designed to comply with the Red Flag Rules promulgated under the Fair and Accurate Credit Transactions Act of 2003 by preventing, detecting, and mitigating identity theft in any accounts offered or maintained by the Company that constitute "covered accounts," as defined by the Red Flag Rules. Therefore, it is mandatory and imperative that Company personnel comply with the policies described herein.

Because the types and methods of identity theft are always evolving and because the Company values and trusts the intelligence and discretion of its personnel to make appropriate decisions in identifying potential indicators of identity theft, the Program retains and incorporates flexibility and discretion at the employee-level. However, the Company has considered and established in the following Program a list of known red flags, which often indicate the possible occurrence of identity theft and a range of potential appropriate responses. The policies outlined below are mandatory and effective immediately. Employees and officers must take appropriate steps to review these policies with and properly train those personnel whose job duties include the intake and review of customer credit and identity information.

Program Officer:

[Name and Title of Program Officer], shall serve as the Program Officer responsible for implementing, overseeing, and administering the Program on an ongoing basis. The Program Officer may designate other employees or representatives of the Company to oversee, administer, or report on particular elements of the Program.

Elements of Program:

This Program applies to any sole proprietor, small business account, or other account offered by or maintained by the Company that involves or is designed to permit multiple payments or transactions. Such accounts include most automobile dealer accounts offered by or maintained by the Company as well as any and all floorplan customers of the Company. It may also include some subscriber accounts. If you have a question about whether a particular type of customer account is covered by the Program, please contact the Program Officer at **[Current Contact Information for the Program Officer]**.

The core element of the Program is to identify those patterns, practices, and specific activities that indicate the potential occurrence of identity theft ("Red Flags") and to highlight, for our personnel and other representatives, appropriate responses to those Red Flags. The Company has reviewed the categories and examples of Red Flags described in the Red Flag Rules, has considered whether other Red Flags may exist, and has identified certain Red Flags that indicate the potential occurrence of identity theft related to customer accounts offered or maintained by the Company. Identified Red Flags are identified herein.

The Program is also designed to oversee identity theft risks that may arise in as direct or indirect consequence of the Company's arrangements with service providers. Whenever the Company engages an external entity (e.g. a service provider) to perform an activity concerning one or more of its covered accounts, the Company should take appropriate measures to ensure that such service provider conducts its activities in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft. Such issues may be addressed in any contract with a service provider.

[If a third-party credentialing service is used by your Company, please include the following italicized paragraph. If no third-party credentialing service is used by your Company, then please omit the following italicized paragraph from this policy.]

Specifically, it is noted that the Company may rely upon customer information gathered and stored by a third-party credentialing service, ***[NAME OF THIRD PARTY SERVICE]*** *("Service"). This information may be used by the Company to register and deal with motor vehicle customers, as well as by the Service for its own purposes. The Service has developed and continues to monitor its own comprehensive identity theft program to protect the information it gathers and stores and has assured the Company that it will diligently implement and oversee its own program.*

This Program also incorporates existing and related Company practices and policies implemented to combat identity theft and other types of fraud.

Red Flags

It is the Company's policy to take all *reasonable* efforts to prevent, detect, and mitigate identity theft in its customer accounts. Although the Company continues to trust the intelligence and discretion of its employees in responding to specific circumstances that may arise, the Company has identified the following "Red Flags" as notable patterns, practices, or specific activities that may indicate the potential existence of identity theft in a customer account offered by or maintained by the Company. Please note that the occurrence or existence of a Red Flag does not necessarily mean that identity theft is occurring. Rather, this list sets forth those issues that the Company would, in most cases, interpret as Red Flags, i.e. signs of potential fraud requiring further inquiry or follow-up.

Employees are expected to take reasonable steps within the ordinary scope of their duties to detect and respond to the following:

1) A credit report received by the Company contains suspicious information, such as:

- A fraud or active duty alert is included with a credit report.
- The Company receives a notice of a credit freeze or other indicator of suspicious activity from a credit reporting agency in response to a request for a credit report.
- A credit reporting agency provides the Company with a notice of an address discrepancy concerning one or more of the Company's customers.
- The Company receives a credit report indicating a pattern of activity that is inconsistent with the known history and usual pattern of activity of an applicant or customer.

2) The Company is presented with suspicious documents relating to a customer, such as:

- Documents provided for identification purposes appear to have been altered or forged.
- The photograph or physical description on an applicant or customer's identification is inconsistent with the appearance of the applicant or customer presenting such identification.
- Other information on the identification is inconsistent with information provided by the person opening a new account or customer presenting the identification.
- Other information on the identification is inconsistent with readily accessible information that is on file with the Company.
- An application or portions thereof appear to have been altered, forged, or destroyed and reassembled.

3) The Company is presented with suspicious personal identifying information relating to a customer, such as:

- Personal identification information provided to the Company is determined to be inconsistent with external information sources the Company utilizes. For example: (i) the address provided does not match an address in the credit report, or (ii) a Social Security Number ("SSN") has not been issued by the government.
- Personal identification information provided by the customer is not consistent with other personal identification information on file with the Company.
- Personal identification information provided to the Company is associated with known fraudulent activity as indicated by internal or third-party sources that may be used by the Company. For example: (i) the address on an application is the same as the address provided on another known fraudulent application, or (ii) the

phone number on an application is the same as the number provided on another known fraudulent application.

- Personal identification information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources that may be used by the Company. For example: (i) the address on an application is fictitious, a mail drop, or a prison, or (ii) the phone number provided is invalid, or is associated with a pager or answering service.

- The SSN provided is the same as that submitted by other persons opening an account or other customers of the Company.

- The address or telephone number provided in the application 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.

- A customer or person opening an account fails either to provide all required personal identification information on an application or respond appropriately to a notification that such application is incomplete.

- When asked for authenticating information, the customer or person opening an account fails to provide such authenticating information or other details about themselves or their business beyond that which generally would be available from a person's wallet or credit report.

- With respect to an account, the Company detects that an incorrect Social Security Number or Employer Identification Number has been provided, that a dealer or individual has requested or opened a duplicate account, that the Company has been provided with altered or otherwise invalid data and/or documentation, that the account holder is deceased, or that an account is missing required data.

- The Company discovers that a customer is not currently in business or that mail sent to a customer is returned to the Company as undeliverable.

4) The Company detects unusual use of, or other suspicious activity related to, an account offered by or maintained by the Company, such as:

- Shortly after receiving a change of address notice concerning an account, the Company receives a request to grant access to such account to additional users.

- An account is used in a manner that is inconsistent with established patterns of activity on the account. Examples of inconsistent activity include, but are not limited to, the following:

  a) Nonpayment when a customer has 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 patters, or

d) A material change in electronic fund transfer or payment patters to or from a deposit account.

- An account that has remained inactive for a long period of time is used (taking into consideration the type of account, the expected pattern of usage, and other relevant factors).
- Mail sent to a customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's account.
- The Company detects, or is otherwise notified that a customer is not receiving Company correspondence, account statements, or other sensitive information sent to customer's address.
- An unknown or unauthorized representative is attempting to conduct business and/or accepts/takes property of a customer.
- The Company detects or is otherwise notified of unauthorized charges or transactions in connection with a customer's account.
- The Company detects or is otherwise notified that a Company employee or contractor has accessed and/or has possession of an unusually large amount and/or atypical type of customer account information, given such employee or contractor's job function or status.
- The Company detects or is otherwise notified of unauthorized charges or transactions in connection with a customer's account.
- The Company detects or is otherwise notified of any unusual change of address activity with respect to an account.

5) Personal Behavior Red Flags

- A customer appears or sounds unusually nervous and/or agitated.
- A customer is unduly pressuring the Company to rush through a transaction.
- A customer or applicant fails or refuses to provide additional information or documentation when requested, particularly in situations involving telephone/internet/email transactions.
- A Company employee or contractor appears unusually nervous and/or agitated if asked about possession or use of customer account information.

- A customer appears unusually disinterested in the price of products or services offered by the Company.

6) The Company receives notice from a customer(s), an alleged victim(s) of identity theft, an auction(s), law enforcement authorities, or other person(s) regarding possible identity theft in connection with an account offered by or maintained by the Company.

Responding to a Red Flag

It is the Company's policy to respond appropriately to all Red Flags upon detection if a reasonable response is likely to prevent, detect, or mitigate identity theft. If an employee detects a Red Flag, he or she should determine the appropriate response by carefully considering all relevant circumstances. The following is a non-exclusive list of potential responses, depending on the specific circumstances:

(a) Monitoring the account for evidence of identity theft,

(b) Contacting the customer for clarification, identity verification, or other information/documentation,

(c) Changing and/or disabling any passwords, security codes, or other security measures that can be used to access an account,

(d) Reopening an account with a new account number,

(e) Not opening an account in response to a new application,

(f) Closing or deactivating an existing account,

(g) Further investigating an individual's identity, which investigation may include the utilization of publicly or commercially available record databases to verify a person's identity,

(h) Notifying one or more affiliated entities that a Red Flag has been detected,

(i) Refusing to release account information if a person cannot provide sufficient proof of identity to demonstrate that such person is entitled to access the account,

(j) Notifying law enforcement or a state governmental entity, and/or

(k) Determining that the particular circumstances or situation warrants no response.

These steps are merely some notable examples of potential responses to a detected Red Flag. Employees should always consider whether other measures or actions are appropriate under the circumstances.

Annual Reports:

The Program Officer or his/her designee shall prepare an annual report (the "Report") regarding the Company's compliance with, and the overall effectiveness of the Program. Such Report shall address material matters related to the Program and evaluate issues such as: the effectiveness of the Program in addressing the risk of identity theft, the Company's efforts to oversee and monitor the identity theft detection, prevention, and mitigation measures undertaken by its service providers, any significant incidents involving identity theft and the Company's response to those incidents, and any recommendations for material changes to the Program. This Report shall be presented to and reviewed by the Program Officer and the Company's President.

Periodic Review of Program:

The Company will periodically review the Program to determine whether changes to the elements of the Program are necessary or warranted. As part of this review, the Company shall consider the methods employed in opening and accessing customer accounts, whether any new or additional Red Flags have been discovered or have otherwise emerged in its business, and whether the Company offers or maintains any additional "covered accounts," as defined by the Red Flag Rules. All material changes to the Program must be approved by the Program Officer.

Acknowledgement of Receipt of Program:

Once you have carefully reviewed the policies described herein, please sign the attached Acknowledgement Form (Exhibit A) and return such to the office of the Program Officer.

Questions or Comments:

If you have any questions, comments, or suggestions about these policies, please contact the office of the Program Officer.

Prepared as guidance for NAAA members – do not use without consulting legal counsel.

EXHIBIT A

PREPARED AS GUIDANCE FOR NAAA MEMBERS – DO NOT USE WITHOUT CONSULTING LEGAL COUNSEL.

Identity Theft Prevention Program
Acknowledgement Form

The undersigned individual acknowledges that he or she has received the Company's Identity Theft Prevention Program, has carefully reviewed and understands the Program, and agrees to comply with the requirements established therein.

_____ (Signature)

_____ (Print Name)

_____ (Date)