MEMORANDUM

TO: **MICHAEL LINN, NIADA EXECUTIVE VICE PRESIDENT/CEO**

FROM: **KEITH WHANN, NIADA General Counsel**

DATE: **July 16, 2008**

RE: **Compliance with the Rules on Identity Theft Red Flags**

The Federal Trade Commission and the federal financial institution regulatory agencies have published final rules on identity theft "red flags" and address discrepancies. The Final Rules implement sections 114 and 315 of the Fair and Accurate Credit Transactions Act of 2003.

The Final Rules require each financial institution and creditor that holds any consumer account, or other account for which there is a reasonably foreseeable risk of identity theft, to develop and implement an Identity Theft Prevention Program (Program) for combating identity theft in connection with new and existing accounts. The Program must include reasonable policies and procedures for detecting, preventing, and mitigating identity theft and enable a financial institution or creditor to:

1. Identify relevant patterns, practices, and specific forms of activity that are "red flags" signaling possible identity theft and incorporate those red flags into the Program;

2. Detect red flags that have been incorporated into the Program;

3. Respond appropriately to any red flags that are detected in order to prevent and mitigate identity theft; and

4. Ensure the Program is updated periodically to reflect changes in identity theft risks.

The agencies also issued guidelines to assist financial institutions and creditors in developing and implementing a Program, including a supplement that provides examples of red flags. The Final Rules require users of consumer reports to develop reasonable policies and procedures to apply when they receive a notice of address discrepancy from a consumer reporting agency.

The final rulemaking was issued by the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Federal Trade Commission, the National Credit Union Administration, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision. The Final Rules became effective on January 1, 2008, with mandatory compliance with the Rules for all covered financial institutions and creditors by November 1, 2008.

We have developed the enclosed materials to assist NIADA Members in complying with the Rules. These materials are being provided to you for distribution to NIADA Members free of charge. We are also providing them to you in electronic format to make it easy for dealers to customize them for their own use. Enclosed you will find:

An Overview Memorandum to Mike Linn of the Red Flags Rules,

A copy of the Rules

Guidelines to assist your dealership in analyzing identity theft red flags and developing a written program,

A model written dealership policy for the detection, prevention and mitigation of identity theft

An employee acknowledgment regarding the Dealership's identity theft program

A service provider agreement addendum regarding the Dealership's identity theft program.

A service provider letter regarding the Dealership's identity theft program.

Please keep in mind that these materials are designed to assist dealers in the development of a written dealership policy for the detection, prevention and mitigation of identity theft and are intended to serve as a guide. While not intended as a universal solution that every dealership can adopt, since they are drafted from a used motor vehicle dealer's perspective, NIADA members should find that they are easy to use and customize for their dealerships. They may wish to consult with their legal counsel or other professional consultants to ensure that their dealership policies are appropriate and in compliance with applicable federal and state laws, rules and regulations. The information contained in this document and the additional materials provided are for general information purposes only and should not be considered as legal advice.

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.

DEALERSHIP IDENTITY THEFT RED FLAGS AND NOTICES OF ADDRESS DISCREPANCY POLICY

This Plan we adopted by _____ (Board of Directors, owner, member, partner, etc.) on _____ (date).

Our Program Coordinator

We have appointed _____ as the Program Coordinator of our Dealership's Identity Theft Red Flags and Notices of Address Discrepancy Policy Program. The Program Coordinator will report to _____, the _____ of the Dealership. In the event the Program Coordinator ceases to be employed by the Dealership or is unable to perform his/her responsibilities, _____ shall assume the responsibilities of the Program Coordinator until a new permanent Program Coordinator is appointed.

The Program Coordinator's Responsibilities

It is the Program Coordinator's responsibility to design, implement and maintain policies and procedures as he/she determines to be necessary from time to time to identify "Red Flags" and notices of address discrepancy as defined the Fact Act of 2003 and the FTC's implementing regulations and as identified in an audit of dealership practices and experience". Specific responsibilities that have been delegated to the Program Coordinator include:

Identifying and assessing the risks of identity theft and discovery of address discrepancies in each relevant area of the Dealership's operation, and evaluating the effectiveness of current safeguards that have been implemented to control these risks and to respond to situations in an appropriate fashion.

Designing and implement policies and procedures that are appropriate for the size and complexity of our Dealership and its operations, the nature and scope of our activities and the sensitivity of the customer information we collect, store and share with others.

Regularly monitoring and testing the policies and procedures for compliance with all applicable law and to determine the effectiveness of our procedure in preventing identity theft.

Assisting with the selection of appropriate service providers that are capable of maintaining safeguards to protect against identity theft and reviewing service provider contracts to ensure that each maintains appropriate procedures for identifying and responding to situations involving identity theft.

Evaluating and adjusting the Dealership's Policy or to a notice of address discrepancy procedure in light of relevant circumstances, including changes to the Dealership's operations, business relationships, technological developments and/or other matters that may impact the security or integrity of th Dealership's customer information and response to identity theft or a notice of address discrepancy.

Pursuant to the Fact Act and the Regulation adopted by the FTC, the Program Coordinator will also be the contact person for Law Enforcement Agencies to communicate possible situations

of identity theft. Upon receiving a request for information from any Law Enforcement Agency, the Program Coordinator will:

Provide the Law Enforcement Agency with his/her name, title, and appropriate contact information, such as a mailing address, e-mail address, telephone number and facsimile number, and notify the Law Enforcement Agency promptly of any modifications with respect to contact information.

If the Dealership has identified possible identity theft or becomes aware of an address discrepancy, the Program Coordinator will send a Report to the customer, as necessary, and to the appropriate Law Enforcement Agency that contains: 1) The name of the individual, entity or organization; 2) The account numbers or, in the case of transactions, the date and type of each transaction; and 3) The Social Security Number, taxpayer identification number, passport number, date of birth, address, or other personal identifying information provided by the individual or entity at the time of the transaction.

Employee Management and Training

All current employees and new hires, as well as independent contractors who provide services to or that perform services on behalf of the Dealership, will:

Be subject to satisfactory reference and consumer/criminal report investigations, where appropriate.

Only have access to customer information if they have a business reason for seeing it.

Participate in the Dealership's privacy policies and information security standards and identity theft and notice of address discrepancy training program and attend education and training seminars on a regular basis, if not otherwise provided for by any independent contractor for its own employees.

Sign and acknowledge his/her agreement to our Dealership's Statement of Privacy Policies; Information Security Standard; Identity Theft and Red Flags; and Notice of Address Discrepancy Policy.

Be responsible for protecting the confidentiality and security of the customer information our Dealership collects and for using the information in accordance with our Policies and Procedures.

Not be permitted to post passwords near their computers or share passwords with any other person.

Refer telephone calls or other requests for customer information to the Program Coordinator or appropriate manager when such requests are not received within the ordinary course of the Dealership's business or are for information that the employee is not authorized to provide.

Disclose to service providers, marketers or any other parties only that customer information which is necessary to complete a transaction initiated by the customer and/or as permitted by law. If an employee is unsure as to whether a specific

disclosure is permitted, he or she will be instructed to check with the Program Coordinator or appropriate manager to verify that it is acceptable to release the information before doing so.

Be required to notify the Program Coordinator or appropriate manager immediately of any attempts by unauthorized persons to obtain access to customer information and/or if any password or customer information is subject to unauthorized access.

Any employee that fails to abide by our Policies and Procedures, whether such failure is intentional or unintentional, will be subject to appropriate disciplinary action, which may include termination of employment.

When an employee ceases to be employed by the Dealership, he/she will be required to turn in any keys in his/her possession that provide access to the Dealership and file cabinets, desks, and offices in the Dealership; passwords and security codes, if applicable, will be deleted; and employees will not be permitted to take any customer information from the Dealership.

Obtaining Customer Information and Verifying Customer identities

The following procedures will be implemented with respect to obtaining customer information and verifying customer identities:

Forms utilized by the Dealership request customer information, such as names, addresses, telephone numbers, birth dates, social security numbers, tax identification numbers, and driver's license and insurance information, to enable the Dealership to verify the identification of its customers. In addition, customers must sign documentation, including sworn statements in some cases, wherein the customer represents and warrants that he/she is the person identified in the documentation.

Employees will request to see the customer's driver's license or other form of government-issued identification bearing a photograph to verify the customer's identity and will make a copy of the same to retain in the customer's file. If a customer requests financing in connection with a transaction, the customer will be required to provide employment information and references and must authorize the Dealership to obtain a credit report, all of which may be utilized to verify the identity of the customer and be used to check for any notice of an address discrepancy. Employees may also request copies of the customer's utility bills, bank or credit card statements and paycheck stubs.

In the event that customer information provided is conflicting or cannot be verified upon further inquiry, employees shall request additional government-issued documentation evidencing the customer's residence and bearing a photograph or other safeguard (i.e. a social security card, alien identification card, or passport) to enable employees to form a reasonable belief that they know a customer's true identity. When appropriate, employees shall write a summary of the means and results of any measures taken to identify a customer, including the resolution of any discrepancy in the identifying information obtained. Employees will be instructed to notify the Program Coordinator if customer information still cannot be verified, or if the employees have obtained information regarding an address discrepancy that cannot be explained.

Paper and electronic records containing customer information and relevant to the Dealership's identity verification process will be retained by the Dealership in accordance with federal and state record retention requirements. Upon the expiration of the appropriate retention period, any such records will be disposed of in a secure manner in accordance with the Dealership's information security standards.

Information Systems

The following information security standards will be implemented in order to protect customer information collected and maintained by our Dealership:

Employees will have access only to that customer information which is necessary to complete their designated responsibilities. Employees shall not have access to or be authorized to provide any other unauthorized person access to customer information that is obtained during the course of employment. Requests for customer information that are outside the scope of the Dealership's ordinary business or the scope of an employee's authorization must be directed to the Program Coordinator or designated individuals.

Access to electronic customer information will be password controlled. Every employee with access to the Dealership's computer system and electronic records will have a unique password consisting of at least _____ characters, including numbers and letters. Only employees that need to access electronic records will be provided with passwords.

All paper and electronic records will be stored in secure locations to which only authorized employees will have access. Any paper records containing customer information must be stored in a deal jacket or folder. Paper records must be stored in an office, desk, or file cabinet that is locked when unattended. Electronic records will be stored on a secure server that is located in a locked room and is accessible only with a password. Where appropriate, records will be maintained in a fireproof file cabinet and/or at an offsite location. Customers, vendors, and service providers shall not be left in an area with insecure customer records.

Backups of the computers and/or server will be made at least once every day, or at more frequent intervals as deemed necessary. At least once each month the backup information will be verified. Backup disks will be stored in a locked file cabinet.

Virus protection software has been installed on the computers and new virus updates will be checked at regular intervals. All computer files will be scanned at least once each month, or at more frequent intervals as deemed necessary.

Firewalls and security patches from software vendors will be downloaded on a regular basis.

All data will be erased from computers, disks, hard drives, or any other electronic media that contain customer information before disposing of them and, where appropriate, hard drives will be removed and destroyed. Any paper records will be shredded and stored in a secure area until an authorized disposal/recycling service picks it up.

Employees will be instructed to log off of all internet, e-mail and other accounts when they are not being used. Employees will not be permitted to download any software or applications to Dealership computers or open e-mail attachments from unknown sources. Electronic records may not be downloaded to a disk or individual computer without explicit authorization from the Program Coordinator.

Electronic records will not be stored online and are not accessible from the internet. If customer information is transmitted electronically over external networks, the information will be encrypted at the time of transmittal.

Neither current nor former employees will be permitted to remove any customer information from the Dealership, whether contained in paper records or electronic records, or to disclose our information security standards to any person without authorization from the Program Coordinator.

Selection and Oversight of Service Providers

In order to protect the customer information our Dealership collects, and to deal with notices of address discrepancies, we will take steps to evaluate and oversee our service providers. The following evaluation criteria will be utilized in selecting service providers:

Compatibility and willingness to comply with the Dealership's policies and procedures and the adequacy of the service provider's own policies and procedures.

Records to be maintained by the service provider and whether the dealership will have access to information maintained by the service provider.

The service provider's knowledge of regulations that is relevant to the services being provided, including privacy, identity theft, and other consumer protection regulations.

Experience and ability to provide the necessary services and supporting technology for current and anticipated needs.

Functionality of any service or system proposed and policies concerning maintaining secure systems, intrusion detection and reporting systems, customer authentication, verification, and authorization, and ability to respond to service disruptions.

Service and support that will be provided in terms of maintenance, security, and other service levels.

Financial stability of the service provider and reputation with industry groups, trade associations, and other dealerships.

Contractual obligations and requirements, such as the term of the contract; prices; software support and maintenance; training of employees; customer service; rights to modify existing services performed under the contract; warranty, confidentiality, indemnification, limitation of liability and exit clauses; guidelines for adding new or different services and for contract re-negotiation; compliance with applicable regulatory requirements; records to be maintained by the service provider; notification of material changes to services, systems, controls and new service locations; insurance coverage

to be maintained by the service provider; and use of the Dealership's data, equipment, and system and application software.

The right of the Dealership to audit the service provider's records, to obtain documentation regarding the resolution of disclosed deficiencies, and to inspect the service provider's facilities.

Service Providers will be required to agree contractually to be responsible for securing and maintaining the confidentiality of customer information, including agreement to refrain from using or disclosing the Dealership's information, except as necessary to or consistent with providing the contracted services, to protect against unauthorized use or disclosure of customer and Dealership information, to comply with applicable privacy and identify theft regulations, and to fully disclose breaches in security resulting in unauthorized access to information that may materially affect the Dealership or its customers and to notify the Dealership to the services provider's corrective action.

Service Providers will be subject to ongoing assessment to evaluate their consistency with selection criteria, performance and financial conditions, and contract compliance.

Managing System Failures

The Program Coordinator will implement audit and oversight procedures as he/she deems necessary to detect the improper disclosure or theft of customer information or notices of any address discrepancy and to ensure that employees, independent contractors, and service providers are complying with our Dealership's Policies and Procedures.

If the Dealership's Identity Theft Policies and Procedures are breached, the Program Coordinator will inform _____, the _____ of the Dealership. The Program Coordinator and _____ will take appropriate steps to notify counsel, service providers, customers, and the appropriate Law Enforcement Agency of any breach, damage or loss of information and the risks associated with the same and will immediately take measures to limit the effect of the breach, identify the reason for the breach and implement procedures to prevent further breaches.

In the event of a breach, or at any other time as the Program Coordinator deems appropriate, the Program Coordinator may modify or supplement our Dealership's Policies and Procedures.

To assist in compliance with applicable state and federal regulations, the Program Coordinator will audit the Dealership's Policies and Procedures at least bi-annually to determine if the current system is operating effectively to prevent/detect identity theft and to deal with notice of any address discrepancy. Any modification of the system that the Program Coordinator deems appropriate will be implemented as soon as reasonably possible.

As part of the audit program, Dealership personnel will be encouraged to advise the Program Coordinator of any newly identified risks to customers or to the safety of the Dealership regarding identity theft. To the extent of any newly identified risk that is discovered, the Program Coordinator is authorized to take appropriate action to address the risk, including assessment, independently or through third parties, of the severity of this risk, and make modifications of the audit system by written instruction to all necessary personnel or through obtaining outside products or services to alleviate the risk.

At leas annually, the Program Coordinator will report to _____(Board of Director, owner, member, partner, etc.) regarding:

1. The effectiveness of the Program

2. Explaining “significant events” involving identity theft and management’s response to any incident

3. Providing recommendations for substantive/material changes to the Policies and Procedures due to evolving risks and methods of identity theft.

ADDENDUM

This Addendum modifies the _____ ("Agreement") entered into between _____ ("Dealer"), and _____ _____ ("Company"), Dealer and Company acknowledge and agree that this Addendum is incorporated into and made a part of the Agreement, the terms and provisions of which, except as expressly modified in this Addendum, are hereby affirmed and ratified by Dealer and Company and remain in full force and effect.

It is agreed between the parties to the Agreement and this Addendum that, notwithstanding anything to the contrary contained in the Agreement or in any other documents pertaining to the Agreement, Dealer and Company shall comply with all identity theft red flag and notice of address discrepancy laws, rules and regulations applicable now and in the future. Without limiting the generality of the proceeding sentence, Dealer and Company agree that they will implement and maintain appropriate safeguards to protect customer's identity information and that they will not use or disclose customer's identity information that they receive pursuant to the terms of this Agreement to any other party, except as is reasonably necessary to fulfill the purposes for which such information was provided and as otherwise permitted by applicable law. The provisions contained in this Addendum shall survive the termination or expiration of the Agreement, by the expiration of time, by operation of law, or otherwise.

IN WITNESS HEREOF, and intending to be bound by the terms and conditions hereof, each of the parties has caused this Addendum to be executed by its duly authorized representative as of the respective dates set forth below.

Dealer: _____	**Company:** _____
Signed: _____	Signed: _____
Print Name: _____	Print Name: _____
Title/Position: _____	Title/Position: _____
Date: _____	Date: _____