COMPANY IDENTITY THEFT RED FLAGS AND NOTICES OF ADDRESS DISCREPANCY POLICY

This Plan we adopted by Star Buick GMC Inc., Star Preowned of Bethlehem LLC, Star Buick GMC Cadillac LLC on January 1, 2019.

Our Program Coordinator

We have appointed Robert P. Grow, Jr. 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 General Manager of the Dealerships. In the event the Program Coordinator ceases to be employed by the Dealership or is unable to perform his responsibilities, the General Manager 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 can maintain 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 the 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 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 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 General Manager of the Dealership. The Program Coordinator and General manager 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 least 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.

I have read and understand the Star Red Flag Policy. (Revised January 2019)

Print Name and Date

_____