Sample Information Security Program

Program Objectives
The objectives of this Information Security Program ("Program") are as follows:

- Insure the security and confidentiality of the Dealership's customer information.
- Protect against any anticipated threats or hazards to the security and/or integrity of the Dealership's customer information.
- Protect against unauthorized access to or use of the Dealership's customer information that could result in substantial harm or inconvenience to any customer.

For purposes of the Program, "customer information" means any information about a customer of the Dealership, or information the Dealership receives about the customer of another financial institution, that can be directly or indirectly attributed to the customer. This Program, in and of itself, does not create a contract between the Dealership and any person or entity.

Program Coordinator(s)
This Program and the safeguards it contemplates shall be implemented and maintained by an employee or employees ("Program Coordinator") designated by the Dealership. The Program Coordinator shall design, implement and maintain new safeguards as he or she determines to be necessary from time to time. The Program Coordinator shall report to the Dealership [*president, managing partner, etc.*] [*and those board members who have responsibility for overseeing the Program.*] The Program Coordinator may delegate or outsource the performance of any function under the Information Security Program as he or she deems necessary from time to time.

In the event the Program Coordinator leaves the employment of the Dealership, the Dealership [*president, managing partner, etc.*] shall take over the responsibilities of the Program Coordinator until a new Program Coordinator is designate.

Risk Assessment
The Program Coordinator shall conduct a risk assessment to identify reasonably foreseeable internal and external risks to the security, confidentiality and integrity of customer information that could result in its unauthorized disclosure, misuse, alteration, destruction or other compromise, and assess the sufficiency of any safeguards in place to control these risks.

The risk assessment shall cover all relevant areas of the Dealership's operations, as determined by the Program Coordinator. At a minimum, the risk assessment shall cover the following:

- Employee training and management;
- Information systems, including network and software design, as well as information processing, storage, transmission and disposal; and

- Detecting, preventing and responding to attacks, intrusions or other systems failures.

Once the Program Coordinator has identified the reasonably foreseeable risks to the Dealership's customer information, the Program Coordinator will determine whether the Dealership's current policies and procedures in these areas sufficiently mitigate the potential risks identified. If not, the Program Coordinator shall design new policies and procedures that meet the objectives of the Program. Final policies and procedures that meet the objectives of the Program shall be made part of the Program.

Audit
The Program Coordinator shall regularly test or audit the effectiveness of the Dealership's safeguards' key controls, systems, and procedures, to ensure that all safeguards implemented as a result of the risk assessment are effective to control the risks identified in the risk assessment. The Program Coordinator shall revise current safeguards and/or implement new safeguards as necessary to ensure the continued viability of the Program.

Overseeing Service Providers
The Program Coordinator shall be responsible for overseeing the Dealership's service providers who handle or have access to customer information. The Program Coordinator shall take reasonable steps to select and retain service providers that are capable of maintaining safeguards to protect the specific customer information handled or accessed by each service provider that are consistent with the level of safeguards employed by the Dealership for such information.

The Program Coordinator shall review and approve each service provider contract prior to its execution by the Dealership to ensure that each contract contains appropriate obligations of the service provider to comply with the Dealership's safeguarding requirements.

Periodic Reevaluation of the Program
The Program Coordinator shall reevaluate and modify the Program from tie to time as the Program Coordinator deems appropriate. The Program Coordinator shall base such reevaluation and modification on the following:

- The results of the Program Coordinator's testing and monitoring efforts;
- Any material changes to the Dealership's operations, business or information technology arrangements; or
- Any other circumstances that the Program Coordinator knows, or has reason to know, may have a material impact of the Program.

In order to assist the Program Coordinator in the regard, the Dealership shall keep the Program Coordinator apprised of the nature and extent of all third party relationships and any operational changes or other matters that may impact the security or integrity of the Dealership's customer information.

Information Security Policies and Procedures – Employee Training and Management

In keeping with the objectives of the Program, the Dealership shall implement, maintain and enforce the following employee management and training safeguards:

[*Insert safeguards appropriate for your Dealership*]

[Safeguards may include the following, as applicable to your Dealership. Note that this is by no means a complete list, nor are the safeguards it contains necessarily appropriate for your Dealership. Ensure your use of any of the following safeguards is consistent with state and local law]:

1. All employees and independent contactors are responsible for complying with the Dealership's Program.
2. The Dealership will check references of each potential employee prior to the commencement of the applicant's employment.
3. The Dealership will obtain a consumer report and criminal background check of each applicant prior to the commencement of the applicant's employment.
4. All offers of employment shall be subject to satisfactory references and consumer/criminal report investigations.
5. All new employees, and independent contractors who perform services in the Dealership, that have access to customer information will participate in the Dealership's information security training. Each person shall sign and acknowledge his or her agreement to abide by the Dealership's Program. Training will recur at least once each year, or sooner, as determined by Dealership management and as required by changes to the Program.
6. Such training program shall include, at a minimum, basic steps to maintain the security, confidentiality and integrity of customer information, such as:

    - Identifying for employees and independent contractors the types of customer information subject to protection under the Information Security Program.
    - 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.
    - Using strong passwords (at least eight characters long and alpha-numeric).
    - Changing passwords periodically, and maintaining the security of passwords.
    - Sending electronic information over secure channels only.
    - Appropriately disposing of paper and electronic records.
    - Other training as determined appropriate by management from time to time.

7. The Dealership will take appropriate steps to encourage awareness of, and compliance with the Program.
8. All employees and independent contractors will be permitted to access customer information on a "need-to-know" basis as determined by Dealership management.
9. Personnel shall not be permitted to access, use or reproduce customer information, whether electronic or non-electronic, for their own use or for any use not authorized by the Dealership.
10. All persons who fail to comply with the Dealership's Program shall be subject to disciplinary measures, up to and including termination of employment for employees or contract termination for independent contractors that perform services with the Dealership. This remedy shall be expressly provided for in Dealer's agreements with such independent contractors.

Information Security Policies and Procedures – Information Systems
In keeping with the objectives of the Program, the Dealership shall implement, maintain and enforce the following information systems safeguards:

[*Insert safeguards appropriate for your Dealership*]

[Safeguards may include the following, as applicable to your Dealership. Note that this is by no means a complete list, nor are the safeguards it contains necessarily appropriate for your Dealership. Ensure your use of any of the following safeguards is consistent with state and local law]:

1. All records containing customer information shall be stored and maintained in a secure area.
    - Paper records shall be stored in a room, cabinet, or other container that is locked when unattended. The Program Coordinator shall control access to such areas.
    - All storage areas shall be protected against destruction or potential damage from physical hazards, like fire or floods.
    - Electronic customer information shall be stored on secure servers. Access to such information shall be password controlled, and the Program Coordinator shall control access to such servers.
    - Customer information consisting of financial or other similar information (e.g., social security numbers, etc.) shall not be stored on any computer system with a direct Internet connection.
    - All customer information shall be backed up on a [insert periodic frequency] basis. Such back up data shall be stored in a secure location as determined by the Program Coordinator.

2. All electronic transmissions of customer information, whether inbound or outbound, shall be performed on a secure basis.

    - Inbound credit card information, credit applications, or other sensitive financial data transmitted to the Dealership directly from consumers shall

use a secure connection, such as a Secure Sockets Layer (SSL) or other currently accepted standard, so that the security of such information is protected in transit. Such secure transmissions shall be automatic. Consumers shall be advised against transmitting sensitive data, like account numbers, via electronic mail.

- The Dealership shall require by contract that inbound transmissions of customer information delivered to the Dealership via other sources be encrypted or otherwise secured.
- All outbound transmissions of customer information shall be secured in a manner acceptable to the Program Coordinator.
- To the extent sensitive data must be transmitted to the Dealership by electronic mail, such transmissions shall be password controlled or otherwise protected from theft or unauthorized access at the discretion of the Program Coordinator.
- The Program Coordinator shall review all vendor applications to ensure an appropriate level of security both within the Dealership and with the Dealership's business partner and vendors.

3. All paper transmissions of customer information by the Dealership shall be performed on a secure basis.
    - Sensitive customer information shall be properly secured at all times.
    - Customer information delivered by the Dealership to third parties shall be kept sealed at all times.
    - Paper-based customer information shall not be left unattended at any time it is in an unsecured area.

4. All customer information shall be disposed of in a secure manner.
    - The Program Coordinator shall supervise the disposal of all records containing customer information.
    - Paper based customer information shall be shredded and stored in a secure area until a disposal or recycling service picks it up.
    - All hard drives, diskette, magnetic tapes, or any other electronic media containing customer information shall be erased and/or destroyed prior to disposing of computers or other hardware.
    - All hardware shall be effectively destroyed.
    - All customer information shall be disposed of in a secure manner after any applicable retention period.

5. The Program Coordinator shall maintain an inventory of Dealership computers, including any handheld devices or PDAs, on or through which customer information may be stored, accessed or transmitted.
6. The Program Coordinator shall develop and maintain appropriate oversight or audit procedures to detect the improper disclosure or theft of customer information.

Information Security Policies and Procedures – Detecting, Preventing and Responding to Attacks, Intrusions or Other Systems Failures

In keeping with the objectives of the Program, the Dealership shall implement, maintain and enforce the following attack and intrusion safeguards:

[*Insert safeguards appropriate for your Dealership*]

[Safeguards may include the following, as applicable to your Dealership. Note that this is by no means a complete list, nor are the safeguards it contains necessarily appropriate for your Dealership. Ensure your use of any of the following safeguards is consistent with state and local law]:

1. The Program Coordinator shall ensure the Dealership has adequate procedures to address any breaches of the Dealership's information safeguards that would materially impact the confidentiality and security of customer information. The procedures shall address the appropriate response to specific types of breaches, including hackers, general security compromises, denial of access to databases and computer systems, etc.
2. The Program Coordinator shall utilize and maintain a working knowledge of widely available technology for the protection of customer information.
3. The Program Coordinator shall communicate with the Dealership's computer vendors from time to time to ensure that the Dealership has installed the most recent patches that resolve software vulnerabilities.
4. The Dealership shall utilize anti-virus software that updates automatically.
5. The Dealership shall maintain up-to-date firewalls.
6. The Program Coordinator shall manage the Dealership's information security tools for employees and pass along updates about any security risks or breaches.
7. The Program Coordinator shall establish procedures to preserve the security, confidentiality and integrity of customer information in the event of a computer or other technological failure.
8. The Program Coordinator shall ensure that access to customer information is granted only to legitimate and valid users.
9. The Program Coordinator shall notify customers promptly if their customer information is subject to loss, damage or unauthorized access.

Information Security Policies and Procedures – [*Insert Operational Area*]

In keeping with the objectives of the Program, the Dealership shall implement, maintain and enforce the following information systems safeguards:

[Insert safeguards appropriate for your Dealership]

* * * * * * * * * *