Klaben Automotive Group, Inc. Information Security Program

Drafted/Adopted: May 15, 2003
Reviewed/Updated by Legal & Management: January 1, 2018

Introduction
The Federal Trade Commission (FTC) Standards for Safeguarding Customer Information (16 CFR Part 314) (the 'Safeguards Rule") applies to parties considered financial institutions within the FTC's jurisdiction under the Gramm-Leach-Bliley (GLB) Act. The Safeguards Rule, effective May 23, 2003, requires those parties to secure records. Klaben Automotive Group, Inc. and its automotive dealerships, Klaben Ford Lincoln, Inc., Klaben Ford Lincoln of Warren, Inc. and Klaben Chrysler Jeep Dodge, Inc. (each dealership is herein referred to as a "Dealership", and collectively, "Klaben") are or may be considered "financial institutions" under the GLB Act and must comply with the provisions of the Act.

Company Policy and Program Objectives
It is the policy of Klaben to comply with the provisions of the Safeguards Rule of the GLB Act. Klaben and its employees will not intentionally share or disclose, or cause to be shared or disclosed, any customer information to any person or entity except where necessary to complete a financial transaction as authorized by the customer. Klaben and its employees will at all times strive to protect and secure all customer information that may be received during the course of a business transaction. Customer information may not be removed from the premises of Klaben without a legitimate business purpose.

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

- Insure the security and confidentiality of Klaben's customer information.
- Protect against any anticipated threats or hazards to the security and/or integrity of Klaben's customer information.
- Protect against unauthorized access to or use of Klaben'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 any Dealership, or information any 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 Klaben and any person or entity. This document describes the Information Security Program which outlines how Klaben and its employees intend to comply with the Act.

Program Coordinator(s)
This Program and the safeguards it contemplates shall be implemented and maintained by certain employees ("Program Coordinators") designated by Klaben Automotive Group, Inc. and each Dealership. The Program Coordinators shall design, implement and maintain new

safeguards as he or she determines to be necessary from time to time. Each Dealership Program Coordinator will report to the President of the Klaben Automotive Group, Inc. The Dealership Program Coordinators 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 any Dealership Program Coordinator leaves the employment of a Dealership, the responsibilities of the Dealership Program Coordinator will be assumed by the other coordinator or coordinators until the new Program Coordinator is appointed.

The Dealership Program Coordinators shall be identified on the schedule attached to this Policy, as the same may be updated from time to time by Klaben management.

Risk Assessment
Each Dealership 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 each Dealership's operations, as determined by the Program Coordinators. 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
- Detecting, preventing and responding to attacks, intrusions, or other system failures

Once the Program Coordinators have 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 Coordinators 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 Coordinators shall review 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 Coordinators shall revise current safeguards and/or implement new safeguards as necessary to ensure the continued viability of the program.

Overseeing Service Providers
The Program Coordinators shall be responsible for overseeing the Dealership's service providers who handle or have access to customer information. The Program Coordinators 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 Coordinators shall review and approve each service provider contract prior to its execution by a 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 Coordinators shall reevaluate and modify the program from time to time as he/she deems appropriate. The Program Coordinators shall base such evaluation and modification on the following:

- The results of the Program Coordinators' testing and monitoring efforts
- Any material changes in the Dealership's operations, business or information technology arrangements
- Any other circumstances that the Program Coordinators know, or have reason to know, may have material impact on the Program

In order to assist in this regard, each Dealership Program Coordinator shall keep the Dealership's President 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 customer information.

Information Security Policies and Procedures – Employee Training and Management
In keeping with the objectives of the Program, each Dealership shall implement, maintain and enforce the following employee management and training safeguards:

1. All employees and independent contractors are responsible for complying with Klaben's Program.
2. Klaben will conduct a criminal background check of each potential employee prior to the commencement of the applicant's employment.
3. All independent contractors that require access to the customer data will sign the Independent Contractor Non-Disclosure agreement prior to accessing the customer data.
4. All new employees who perform services in a 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. For persons whose jobs require them to access customer information, training will recur at least once each year, or sooner, as determined by Dealership management and as required by changes to the Program.
5. Such training program shall include, at a minimum, basic steps to maintain security, confidentiality and integrity of customer information, such as:
    - Identifying for employees the types of customer information subject to protection under the Information Security Program.
    - Securing 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.
    - Maintaining the security of passwords.
    - Periodically updating passwords to reduce the risk of theft and/or breach.
    - Password protecting all mobile devices with access to electronic mail or other electronic records which may contain customer information.
    - Reporting suspicious call, e-mails, and other inquiries requesting customer information or other confidential information to the Information Security Program Coordinators or designated contacts.
    - Sending electronic information over secure channels only.
    - Appropriately disposing of paper and electronic records.
    - Other training as determined by management from time to time.
6. The Dealership will take appropriate steps to encourage awareness of, and compliance with, the Program.

7. All employees and independent contractors will be permitted to access customer information on a "need-to-know" basis as determined by Dealership management.
8. 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.
9. 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 and contract termination for independent contractors that perform services in the Dealership.

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:

1. All records containing customer information shall be stored and maintained in a secure area.
   - Inactive paper records, such as completed deal files, shall be secured in rooms that are either locked or subject to controlled access in non-public areas.
   - Active paper records, such as deals in process, shall be stored in locked files or otherwise secured in non-public areas.
   - Electronic customer information shall be stored on secure servers. Access to such information shall be password controlled, and the Dealership Program Coordinators 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 an unprotected internet connection.
   - Customer information will be backed up as part of our complete daily computer file back up process. Such back up data shall be stored in a secure location as determined by the Dealership Program Coordinators.
2. All electronic transmissions of customer information, whether inbound or outbound, shall be performed on a secure basis.
   - The Dealership shall require that inbound transmissions of customer information delivered to the dealership in a secure manner acceptable to the Dealership Program Coordinators.
   - All outbound transmissions of customer information shall be secured in a manner acceptable to the Dealership 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 Dealership Program Coordinators.
   - The Dealership Program Coordinators shall review all vendor applications to ensure an appropriate level of security both within the Dealership and with the Dealership's business partners and vendors.
3. All paper transmissions of customer information by the Dealership shall be performed on a secure basis.
   - Sensitive customer information shall be secured at all times.
   - Customer information delivered by the Dealership to third parties shall be transported in a secure manner by being sealed in a delivery company provided container or personally delivered by a Dealership employee.
   - Paper-based customer information shall not be left unattended at any time it is in an unsecured area.
4. All customer information will be disposed of in a secure manner.

- Each Dealership Program Coordinator shall supervise the disposal of all bulk stored records containing customer information.
- Paper based customer information shall be shredded as the preferred means of disposal after any applicable retention period has expired.
- All hard drives, diskettes, 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 will be effectively destroyed.

5. Each Dealership 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.

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

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

1. The Program Coordinators shall utilize and maintain a working knowledge of widely available technology for the protection of customer information.
2. Each Dealership 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.
3. Each Dealership shall maintain up-to-date firewalls and antivirus software.
4. Each Dealership Program Coordinator shall utilize tools and processes established by the Dealership software vendor to preserve the security, confidentiality and integrity of customer information in the event of a computer or other technological failure.
5. Each Dealership Program Coordinator shall ensure that access to customer information is granted only to legitimate and valid users.
6. Each Dealership Program Coordinator shall notify customers promptly if their customer information becomes subject to loss, damage or unauthorized access.

Program Coordinators: Updated August 1, 2020 Klaben Automotive Group, Inc.

Program Coordinator	Heather Knapp	330-673-3139
Program Coordinator	Tracy Tucci	330-673-3139
Program Coordinator	Roger Parsons	330-369-4444
Program Coordinator	Carla Caskey	330-677-2888