# COMPLIANCE WITH THE FEDERAL TRADE COMMISSION'S SAFEGUARDS RULE

# COMPLIANCE WITH THE FEDERAL TRADE COMMISSION'S SAFEGUARDS RULE

Most dealers are familiar with the requirements of the Gramm-Leach-Bliley Act and the Federal Trade Commission's (FTC) Privacy Rule, which obligate them to create and distribute Privacy Notices to their customers. What they may not know is that the FTC's Standards for Safeguarding Customer Information, more commonly known as the "Safeguards Rule," becomes effective on May 23, 2003. The objectives of the Safeguards Rule are to insure the security and confidentiality of customer information, protect against any anticipated threats or hazards to the security and integrity of customer information, and protect against unauthorized access to or use of customer information that could result in substantial harm or inconvenience to a customer.

The FTC's Safeguards Rule does not change the dealership's obligations under the FTC's Privacy Rule. The Privacy Rule deals with how financial institutions collect and share information. Motor vehicle dealerships are still required to provide their customers with a Privacy Notice that advises the customer about the types of information the dealership collects, the sources from which the information may be obtained and the dealership's policies with respect to sharing that information. As you may recall, in order to fully comply with the Gramm-Leach-Bliley Act and the FTC's Privacy Rule, motor vehicle dealers were also required to make a statement about their information safeguarding practices in their Privacy Notices. As a result, most dealership Privacy Notices state "we maintain physical, electronic and procedural safeguards to protect the confidentiality and security of the information we collect". Now the Safeguards Rule mandates that dealers have a written document that specifies the steps they have taken to assess the types of risks that exist with respect to the information being obtained by unauthorized individuals and to protect the confidentiality and security of such information.

Like the Privacy Rule, the Safeguards Rule applies only to transactions involving persons who obtain a financial product or service from the dealership primarily for personal, family or household purposes. Although it is a good idea to apply the same privacy policies and information security standards to all of the information collected by the dealership, it is not required for information about companies or individuals who obtain financial products or services for business, commercial or agricultural purposes, unless the dealership's Privacy Notice states otherwise. Personal information typically collected from customers at the dealership includes their names, addresses, telephone numbers, birth dates and social security numbers, information contained in credit applications and credit reports, information dealerships receive from lenders, and even lists of the dealership's finance customers.

The FTC's Safeguards Rule specifically requires every dealer, regardless of the size of his dealership, to develop, implement and maintain a comprehensive written information security plan that describes the dealership's program to protect customer information. It also requires them to ensure that affiliates of the dealership maintain appropriate safeguards and that their service providers are capable of maintaining appropriate safeguards for the customer information the dealership shares. The Dealership's written information security plan must: (1) Designate an employee or employees to coordinate the safeguards; (2) Identify and assess the risks to customer information in each relevant area of the dealership's operation, and evaluate the effectiveness of the current safeguards for controlling these risks; (3) Design and implement a safeguards program, and regularly monitor and test it; (4) Select appropriate service providers and contract with them to implement safeguards; and (5) Evaluate and adjust the program in light of relevant circumstances, including changes in business arrangements or operations, or the results of testing and monitoring of safeguards.

When we filed comments regarding the Safeguards Rule on behalf of NIADA, we requested that the FTC adopt flexible requirements, and the FTC did just that. The dealership's privacy policies and information security standards must be developed taking into consideration the dealership's size and complexity, the nature and scope of its activities, the sensitivity of the information it collects, and theses policies and standards must be regularly monitored. When implementing the Safeguards Rule, the dealership must consider all areas of its operation, including three that are particularly important to information security: Employee management and training; information systems, and managing system failures. In an effort to help businesses understand and comply with the FTC's Financial Information Safeguards Rule, the FTC issued a new "Facts for Business" Publication titled "Financial Institutions and Customer Data: Complying with the Safeguards Rule."

While compliance with the FTC's Safeguards Rule is just around the corner and, therefore, on the top of everyone's agenda, dealers are well advised to consider other Federal Privacy and Anti-Terrorism Laws that have recently been enacted or are under consideration. For example, on October 26, 2001, the President signed into law the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA Patriot Act). Title III of the USA Patriot Act makes a number of amendments to the anti-money laundering provisions of the Bank Secrecy Act (BSA) that are intended to promote the prevention, detection, and prosecution of international money laundering and the financing of terrorism. Under the USA Patriot Act, the term "financial institution" is defined to include a "business engaged in vehicle sales, including automobile, airplane, and boat sales."

The Treasury Department has already issued a Final Rule implementing Section 314 of the USA Patriot Act, which establishes procedures that encourage information sharing between governmental authorities and financial institutions, and among financial institutions themselves. The first part of the Rule establishes a mechanism for law enforcement agencies to communicate the names of suspected terrorists and money launders to financial institutions in an effort to locate and secure accounts and transactions involving those suspects. Effective as of September 26, 2002, any motor vehicle dealerships that receive the name of a suspect must designate one person at the dealership to be the contact person regarding the request and any future requests that it receives. They must also establish adequate procedures to protect the security and confidentiality of the requests received from FinCEN and their responses to these requests. The requirement to maintain adequate security and confidentiality procedures to protect the information is met if the dealership applies the same procedures it has established to comply with the Gramm-Leach-Bliley Act and the FTC's Safeguards Rule.

The USA Patriot Act also requires every financial institution to establish an anti-money laundering program. Pursuant to Section 352 of the Act, the anti-money laundering program must include, at a minimum: (1) The development of internal policies, procedures, and controls; (2) The designation of a compliance officer; (3) An ongoing employee-training program; and (4) An independent audit function to test programs. Section 326 of the Act further requires the Treasury to prescribe Regulations setting forth minimum standards for financial institutions to identify customers applying to open accounts, including: (1) Adopting reasonable procedures for verifying the identity of any person seeking to open an account; (2) Maintaining records of the information used to verify the person's identity, including the person's name, address, and other identifying information; and (3) Determining whether the person appears on any lists of known or suspected terrorists or terrorist organizations provided to the financial institution by a Government Agency. Although motor vehicle dealers have been temporarily exempted from the requirement to establish an anti-money laundering compliance program, on February 24, 2003, FinCEN published an Advance Notice of Proposed Rulemaking to solicit public comments as to how these requirements should apply to motor vehicle dealers.

To eliminate the need for NIADA Members to draft new or modified privacy policies and information security standards in the future, we have developed the enclosed materials to assist them in complying not only with the FTC's Safeguards Rule, but also with the USA Patriot Act and emerging implementing regulations that will impact every dealership's policies, practices and overall operations. 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 the:

- FTC Guidelines titled "Financial Institutions and Customer Data: Complying with the Safeguards Rule," which summarize the purpose for the Safeguards Rule and include suggested policies and procedures for complying with the Rule.

- Program Coordinator's Audit of Dealership Privacy Policies and Information Security Standards Checklist

- Dealership Privacy Policies and Information Security Standards

- Employee Agreement to Comply with Privacy Policies and Information Security Standards

- Statement of Privacy Policies and Information Security Standards

- Addendum to Service Provider Agreements and Letter to Service Providers Regarding Safeguarding Information

Please keep in mind that these materials are designed to assist dealers to identify and implement appropriate policies and standards for protecting customer information. They are intended as a guide for motor vehicle dealers to develop their privacy policies and information security standards. 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. It is important that dealers be instructed to familiarize themselves will all of the information contained in the documents provided and include only those privacy policies and information security standards that are feasible for the dealership to implement and maintain. In addition, there may be state specific data protection or safeguards rules with which dealers must comply and, therefore, they may wish to consult with their legal counsel or other professional consultants to ensure that their privacy policies and information security standards are appropriate for the dealership 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.

BUSINESS

FOR THE CONSUMER www.ftc.gov

FEDERAL TRADE COMMISSION 1-877-FTC-HELP

# FTC FACTS for Business

# Financial Institutions and Customer Data: Complying with the Safeguards Rule

Many financial institutions collect personal information from their customers, such as their names, addresses and phone numbers; bank and credit card account numbers; income and credit histories; and Social Security numbers. The Gramm-Leach-Bliley (GLB) Act requires financial institutions to ensure the security and confidentiality of this type of information.

As part of its implementation of the GLB Act, the Federal Trade Commission (FTC) has issued the Safeguards Rule. This Rule requires financial institutions under FTC jurisdiction to secure customer records and information.

## Who Must Comply

The Safeguards Rule applies to businesses, regardless of size, that are "significantly engaged" in providing financial products or services to consumers. This includes check-cashing businesses, data processors, mortgage brokers, nonbank lenders, personal property or real estate appraisers, professional tax prepares, courier services, and retailers that issue credit cards to consumers. The Safeguards Rule also applies to financial companies, like credit reporting agencies and ATM operators, that receive information from other financial institutions about their customers. In addition to developing their own safeguards, financial institutions are responsible for taking steps to ensure that their affiliates and service providers safeguard customer information in their care.

The Safeguards Rule is posted at **www.ftc.gov/privacy/glbact**. To find out whether your company is a financial institution, check section 313.3(k) of the FTC's Privacy Rule and related materials at **www.ftc.gov/privacy/glbact**.

## An Added Value

Adequately securing customer information is not only the law, it makes good business sense. When you show customers that you care about the security of their personal information, you increase their level of confidence in your institution. Poorly-managed customer data can lead to identity theft. Identity theft occurs when someone steals a consumer's personal identifying information to open new charge accounts, order merchandise or borrow money.

## How to Comply

The Safeguards Rule requires financial institutions to develop a written information security plan that describes their program to protect customer information. The plan must be appropriate to the financial institution's size and complexity, the nature and scope of its activities, and the sensitivity of the customer information it handles. As part of its plan, each financial institution must:

1. designate one or more employees to coordinate the safeguards;
2. identify and assess the risks to customer information in each relevant area of the company's operation, and evaluate the effectiveness of the current safeguards for controlling these risks;
3. design and implement a safeguards program, and regularly monitor and test it;
4. select appropriate service providers and contract with them to implement safeguards; and
5. evaluate and adjust the program in light of relevant circumstances, including changes in the firm's business arrangements or operations, or the results of testing and monitoring of safeguards.

These requirements are designed to be flexible. Each financial institution should implement safeguards appropriate to its own circumstances. For example, some financial institutions may choose to describe their safeguards programs in a single document, while others may memorialize their plans in several different documents, such as one to cover an information technology division and another to describe the training program for employees. Similarly, a company may decide to designate a single employee to coordinate safeguards or may spread this responsibility among several employees who will work together.

In addition, a firm with a small staff may design and implement a more limited employee training program than a firm with a large number of employees. And a financial institution that doesn't receive or store any information online may take fewer steps to assess risks to its computers than a firm that routinely conducts business online.

## Securing Information

When a firm implements safeguards, the Safeguards Rule requires it to consider all areas of its operation, including three areas that are particularly important to information security: **employee management and training**; **information systems**; and **managing system failures**. Firms should consider implementing the following practices in these areas.

### Employee Management and Training

The success or failure of your information security plan depends largely on the employees who implement it. You may want to:

- Check references prior to hiring employees who will have access to customer information.
- Ask every new employee to sign an agreement to follow your organization's confidentiality and security standards for handling customer information.
- Train employees to take basic steps to maintain the security, confidentiality and integrity of customer information, such as:
  - locking rooms and file cabinets where paper records are kept;
  - using password-activated screensavers;
  - using strong passwords (at least eight characters long);
  - changing passwords periodically, and not posting passwords near employees' computers;
  - encrypting sensitive customer information when it is transmitted electronically over networks or stored online;
  - referring calls or other requests for customer information to designated individuals who have had safeguards training; and
  - recognizing any fraudulent attempt to obtain customer information and reporting it to appropriate law enforcement agencies.
- Instruct and regularly remind all employees of your organization's policy — and the legal requirement — to keep customer information secure and confidential. You may want to provide employees with a detailed description of the kind of customer information you handle (name, address, account number, and any

other relevant information) and post reminders about their responsibility for security in areas where such information is stored — in file rooms, for example.
- Limit access to customer information to employees who have a business reason for seeing it. For example, grant access to customer information files to employees who respond to customer inquiries, but only to the extent they need it to do their job.
- Impose disciplinary measures for any breaches.

## Information Systems

Information systems include network and software design, and information processing, storage, transmission, retrieval, and disposal. Here are some suggestions on how to maintain security throughout the life cycle of customer information — that is, from data entry to data disposal:

- Store records in a secure area. Make sure only authorized employees have access to the area. For example:
  - store paper records in a room, cabinet, or other container that is locked when unattended;
  - ensure that storage areas are protected against destruction or potential damage from physical hazards, like fire or floods;
  - store electronic customer information on a secure server that is accessible only with a password — or has other security protections — and is kept in a physically-secure area;
  - don't store sensitive customer data on a machine with an Internet connection; and
  - maintain secure backup media and keep archived data secure, for example, by storing off-line or in a physically-secure area.
- Provide for secure data transmission (with clear instructions and simple security tools) when you collect or transmit customer information. Specifically:
  - if you collect credit card information or other sensitive financial data, use a Secure Sockets Layer (SSL) or other secure connection so that the information is encrypted in transit;
  - if you collect information directly from consumers, make secure transmission automatic. Caution consumers against transmitting sensitive data, like account numbers, via electronic mail; and
  - if you must transmit sensitive data by electronic mail, ensure that such messages are password protected so that only authorized employees have access.
- Dispose of customer information in a secure manner. For example:
  - hire or designate a records retention manager to supervise the disposal of records containing nonpublic personal information;
  - shred or recycle customer information recorded on paper and store it in a secure area until a recycling service picks it up;
  - erase all data when disposing of computers, diskettes, magnetic tapes, hard drives or any other electronic media that contain customer information;
  - effectively destroy the hardware; and
  - promptly dispose of outdated customer information.
- Use appropriate oversight or audit procedures to detect the improper disclosure or theft of customer information. For example, supplement each of your customer lists with at least one entry (such as an account number or address) that you control, and monitor use of this entry to detect all unauthorized contacts or charges.
- Maintain a close inventory of your computers.

## Managing System Failures

Effective security management includes the prevention, detection and response to attacks, intrusions or other system failures. Consider the following suggestions:

- Maintain up-to-date and appropriate programs and controls by:
  - following a written contingency plan to address any breaches of your physical, administrative or technical safeguards;

  - checking with software vendors regularly to obtain and install patches that resolve software vulnerabilities;
  - using anti-virus software that updates automatically;
  - maintaining up-to-date firewalls, particularly if you use broadband Internet access or allow employees to connect to your network from home or other off-site locations; and
  - providing central management of security tools for your employees and passing along updates about any security risks or breaches.
- Take steps to preserve the security, confidentiality and integrity of customer information in the event of a computer or other technological failure. For example, back up all customer data regularly.
- Maintain systems and procedures to ensure that access to nonpublic consumer information is granted only to legitimate and valid users. For example, use tools like passwords combined with personal identifiers to authenticate the identity of customers and others seeking to do business with the financial institution electronically.
- Notify customers promptly if their nonpublic personal information is subject to loss, damage or unauthorized access.

## For More Information

Additional guidance is available at **www.ftc.gov/privacy/glbact** and **www.ftc.gov/infosecurity**. Resources at these sites may alert you to new risks to information security and help those individuals whose information may have been compromised with their next steps. In addition, the following organizations have information available to help you implement appropriate safeguards for your customer data.

- Computer Security Resource Center, The National Institute for Standards and Technology (NIST) — **www.csrc.nist.gov**
- Critical Infrastructure Assurance Office (CIAO) — **www.ciao.gov**
- Federal Deposit Insurance Corporation (FDIC) — **www.fdic.gov**
  *Tools to Manage Technology Providers' Performance Risk: Service Level Agreement* — **www.fdic.gov/regulations/information/btbulletins/brochure2.html**
  *Effective Practices for Selecting a Service Provider* — **www.fdic.gov/regulations/information/btbulletins/brochure1.html**
- National Infrastructure Protection Center (NIPC) — **www.nipc.gov**
  *Seven Simple Computer Security Tips for Small Business and Home Computer Users* — **www.nipc.gov/publications/nipcpub/computertips.htm**
- System Administration, Networking and Security Institute (SANS) — **www.sans.org**
  *The 20 Most Critical Internet Security Vulnerabilities* — **www.sans.org/top20.htm**

The FTC works for the consumer to prevent fraudulent, deceptive and unfair business practices in the marketplace and to provide information to help consumers spot, stop and avoid them. To file a complaint or to get free information on consumer issues, visit www.ftc.gov or call toll-free, 1-877-FTC-HELP (1-877-382-4357); TTY: 1-866-653-4261. The FTC enters Internet, telemarketing, identity theft and other fraud-related complaints into Consumer Sentinel, a secure, online database available to hundreds of civil and criminal law enforcement agencies in the U.S. and abroad.

## Your Opportunity to Comment

The Small Business and Agriculture Regulatory Enforcement Ombudsman and 10 Regional Fairness Boards collect comments from small business about federal enforcement actions. Each year, the Ombudsman evaluates enforcement activities and rates each agency's responsiveness to small business. To comment on FTC actions, call 1-888-734-3247.

**PROGRAM COORDINATOR'S AUDIT OF DEALERSHIP PRIVACY POLICIES AND INFORMATION SECURITY STANDARDS CHECKLIST**

**Employee Management and Training**

- Are current employees, new hirees and independent contractors who perform services on behalf of the Dealership subject to satisfactory reference and, where appropriate, consumer/criminal report investigations?

- Have you developed processes that limit access to customer information and other confidential records to authorized employees?

- Do you have a written document outlining the policies and procedures for handling confidential information?

- Have you considered having employees formally acknowledge their understanding of information security policies and practices?

- What steps has the Dealership taken to train employees on its privacy policies and information security standards?

- Does the Dealership employ password-protection software and encryption programs as appropriate and have employees been advised not to post passwords near their computers or share passwords with any other person?

- Do you have appropriate disciplinary policies?

- When an employee ceases to be employed by the Dealership, do you delete outdated user names and passwords from electronic databases and networks and obtain all keys to the Dealership and file cabinets, desks, and offices in the Dealership from the employee?

- Have you contacted your Dealer Association, Legal Professionals or other consultants to assist you with compliance as necessary?

**Obtaining Customer Information and Verifying Customer Identities**

- Do your forms request adequate customer information to verify the identity of the Dealership's customers?

- Do employees request to see the customer's driver's license or other form of government-issued identification with a photograph to verify the customer's identity?

- What policies does the Dealership have in place to address situations when customer information is conflicting or cannot be verified?

- Do you have procedures for ensuring that the Dealership does not enter into transactions with individuals or entities that appear on the list of Specially Designated Nationals and Blocked Persons maintained by the Office of Foreign Asset Control (OFAC)?

- Do you have record retention policies for files that contain customer information and identity verification?

**Information Systems**

- How do you secure records?

- Are records that contain customer information stored where they can be locked when unattended?

- Are file cabinets, desk drawers and offices locked securely?

- Are storage areas secure from unauthorized access and protected against physical hazards like fire or floods?
- What is the process for collecting and filing written records?
- Are your electronic records stored securely?
- Do the passwords you assign contain enough characters and consist of both letters and numbers?
- Is on-screen information protected?
- Do you change passwords periodically and require employees to keep them private?
- How do you transmit and receive sensitive customer information?
- What measures are taken when disposing of customer information?
- Do you shred documents containing customer information and store it in a secure area until an authorized disposal/recycling service picks it up?
- How do you ensure data is eliminated when disposing of computers, disks, hard drives or any other electronic media that contains customer information?
- Is there a need for a designated records retention manager?
- Is it necessary to establish retention periods for written customer files?
- Are employees prohibited from taking customer information out of the Dealership?
- How do you make sure your anti-virus and firewall software is up-to-date?
- Do you have a system for backing up information on computers and/or servers?
- Are employees instructed to log off of all Internet, E-mail and other accounts when they are not being used?
- Who is responsible for downloading software or applications to the Dealership's computers?
- Have you taken steps to prevent and prepare for a systems failure?

**Selection and Oversight of Service Providers**

- Have you established criteria for evaluating, selecting and auditing service providers?
- Does the Dealership have contractual agreements with all of its service providers?
- Are service providers required to agree to be responsible for securing and maintaining the confidentiality of customer information?
- Is the Dealership advised when a security breach occurs and does the Dealership have policies of advising it's service providers of security breaches?

**Managing System Failures**

- Do you have a system for auditing and overseeing the Dealership's privacy policies and information security standards?

- Does the Dealership take immediate corrective action when a security breach occurs?

# DEALERSHIP PRIVACY POLICIES AND INFORMATION SECURITY STANDARDS

## Our Program Coordinator

We have appointed _____ as the Program Coordinator of our Dealership's Information Security Program. The Program Coordinator will report directly 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 take over 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 privacy policies and information safeguard standards as he/he determines to be necessary from time to time. Specific responsibilities that have been delegated to the Program Coordinator include:

Identifying and assessing the risks to customer information in each relevant area of the Dealership's operation, and evaluating the effectiveness of current safeguards that have been implemented to control these risks.

Designing and implementing privacy policies and information security standards 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 privacy policies and information security standards.

Assisting with the selection of appropriate service providers that are capable of maintaining safeguards to protect the relevant customer information and reviewing service provider contracts to ensure that each contracts contain appropriate obligations with respect to the use of customer information and the implementation of safeguards.

Evaluating and adjusting the Dealership's Privacy Policies and Information Security Standards 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.

Pursuant to the USA Patriot Act and the Rules adopted by the Financial Crimes Enforcement Network (FinCEN), a Bureau under the Department of Treasury, the Program Coordinator will also be the contact person for Law Enforcement Agencies to communicate the names of suspected terrorists and money launders in an effort to locate and secure accounts and transactions involving those suspects. Upon receiving a request for information from FinCEN, the Program Coordinator will:

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

Ensure that current accounts maintained by the Dealership, any accounts maintained by the Dealership during the past 12 months, and any transactions conducted during the past 6 months that the Dealership is required by law or regulation to record or that the Dealership has recorded and maintained are searched for the names provided by FinCEN.

If the Dealership has entered into a transaction with an individual or entity on the list, send a Report to FinCEN 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.

Questions about the scope or terms of a request will be directed to the Law Enforcement Agency that sent the request for information to FinCEN, but the Report will be sent to FinCEN, not the Law Enforcement Agency that requested the search, unless the Program Coordinator is instructed otherwise.

**Employee Management and Training**

All current employees and new hirees, as well as independent contractors who 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 training program and attend educational and training seminars on a regular basis.

Sign and acknowledge his/her agreement to our Dealership's Statement of Privacy Policies and Information Security Standards.

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

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 Statement of Privacy Policies and Information Security Standards, 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. 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 in documentation 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.

The Dealership has access to updated versions of the alphabetical master list of Specially Designated Nationals and Blocked Persons maintained by the Office of Foreign Asset Control (OFAC), which will be checked to ensure that potential customers do not appear on the same.

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 access or 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 each 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, employees will be instructed to encrypt the information 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, 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 privacy policies and information security standards and the adequacy of the service provider's own privacy policies and information security standards.

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 are relevant to the services being provided, including privacy 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 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 of 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 and to ensure that employees, independent contractors and service providers are complying with our Dealership's Privacy Policies and Information Security Standards.

If the Dealership's Privacy Policies and Information Security Standards are breached, the Program Coordinator will inform _____, the _____ of the Dealership. The Program Coordinator and _____will take appropriate steps to notify counsel, service providers and customers 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 Privacy Policies and Information Security Standards.

# EMPLOYEE AGREEMENT TO COMPLY WITH PRIVACY POLICIES AND INFORMATION SECURITY STANDARDS

Effective July 1, 2001, the Financial Services Modernization Act of 1999, more commonly know as the "Gramm-Leach-Bliley Act", requires "financial institutions" that collect nonpublic personal information about customers who obtain a "financial product or service" to: (1) Implement privacy policies and procedures to protect the information they collect; and (2) Provide their customers with certain notices, including an Initial Privacy Policy Notice and, if applicable, an Annual Notice. In addition, as of May 23, 2003, any financial institution that collects personal information from their customers must comply with the Federal Trade Commission's Safeguards Rule, which requires financial institutions to develop a written information security plan that describes their program to protect customer information. In certain circumstances, our Dealership is deemed to be a "financial institution" for purposes of the Gramm-Leach-Bliley Act and the Federal Trade Commission's Implementing Rules. As a condition of your employment with our Dealership, you agree to:

1. Read the "Statement of Privacy Policies and Information Security Standards" and familiarize yourself with the information contained therein.

2. Follow our procedures for providing a copy of our Privacy Policy to each customer.

3. Follow our procedures for safeguarding and protecting customer information in accordance with our "Statement of Privacy Policies and Information Security Standards".

**BY SIGNING BELOW, I ACKNOWLEDGE THAT I HAVE RECEIVED AND READ THE STATEMENT OF PRIVACY POLICIES AND INFORMATION SECURITY STANDARDS AND AGREE TO COMPLY WITH THE PRIVACY POLICIES AND INFORMATION SECURITY STANDARDS AS SET FORTH THEREIN AS A CONDITION OF MY EMPLOYMENT. I FURTHER UNDERSTAND THAT THE FAILURE TO FOLLOW THE DEALERSHIP'S PRIVACY POLICIES AND INFROMATION SECURITY STANDARDS MAY RESULT IN DISCIPLINARY ACTION, INCLUDING THE TERMINATION OF MY EMPLOYMENT.**

_____ _____

EMPLOYEE DATE

_____ _____

WITNESS DATE

# STATEMENT OF PRIVACY POLICIES AND INFORMATION SECURITY STANDARDS

Effective July 1, 2001, the Financial Services Modernization Act of 1999, more commonly know as the "Gramm-Leach-Bliley Act", requires "financial institutions" that collect nonpublic personal information about customers who obtain a "financial product or service" to: (1) Implement privacy policies and procedures to protect the information they collect; and (2) Provide the customers with certain notices, including an Initial Privacy Policy Notice and, if applicable, an Annual Notice. In addition, as of May 23, 2003, any financial institution that collects personal information from their customers must comply with the Federal Trade Commission's Safeguards Rule, which requires financial institutions to develop a written information security plan that describes their program to protect customer information. In certain circumstances, our Dealership is deemed to be a "financial institution" for purposes of the Gramm-Leach-Bliley Act and the Federal Trade Commission's Implementing Rules. The purpose of this Statement is to advise you of your responsibilities as an Employee of our Company. As a condition of your employment with our Dealership, you agree to:

1. Read this "Statement of Privacy Policies and Information Security Standards" and familiarize yourself with the information contained herein.

2. Follow our procedures for providing a copy of our Privacy Policy to each customer.

3. Follow our procedures for safeguarding and protecting customer information in accordance with our Information Security Standards.

## OUR PRIVACY POLICY

Employee are responsible for providing a copy of our Privacy Policy to each customer:

1. That enters into an agreement or understanding for assistance to obtain a loan or financing, regardless of whether or not financing is ever obtained, as follows:

   a. In person when the customer completes a Credit Application;

   b. By mail within _____ day(s) of receipt of the information to complete a Credit Application via the telephone;

2. When information is collected in order to assist the customer to obtain payoff information on a trade-in vehicle; and

3. That purchases other products or services (i.e. service contracts, guaranteed automobile protection (GAP) agreements or insurance) prior to completion of the sale or lease transaction.

## OUR INFORMATION SECURITY STANDARDS

### Our Program Coordinator

We have appointed _____ as the Program Coordinator of our Dealership's Information Security Program. It is the Program Coordinator's responsibility to design, implement and maintain privacy policies and information safeguard standards as he/he determines to be necessary from time to time. The Program Coordinator will report directly 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 take over the responsibilities of the Program Coordinator until a new permanent Program Coordinator is appointed.

Based upon the Program Coordinator's risk assessment of our Dealership's operations, including employee management and training and our information systems (i.e. information collection, processing, storage, transmission and disposal, and potential system failures), the following privacy policies and information security standards have been adopted for all of our employees and any independent contractors. Individual employees may be given additional responsibilities as well. Compliance with our Dealership's privacy policies and information security standards is a condition of your employment with us.

**Employee Interviewing, Hiring and Training**

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

1. Be subject to satisfactory reference and consumer/criminal report investigations.

2. Participate in the Dealership's privacy policies and information security standards training program and attend educational and training seminars on a regular basis.

3. Sign and acknowledge his/her agreement to our Dealership's Statement of Privacy Policies and Information Security Standards.

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

**Obtaining Customer Information and Verifying Customer Identities**

The following procedures have been implemented with respect to obtaining customer information and verifying customer identities:

1. 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.

2. Employees must 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 must complete a credit application, provide employment information and references, and authorize the Dealership to obtain a credit report. Employees may also request copies of the customer's utility bills, bank or credit card statements and paycheck stubs.

3. In the event that customer information provided in documentation 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. If customer information still cannot be verified, employees shall notify the Program Coordinator for further instructions.

4. The Dealership has access to updated versions of the alphabetical master list of Specially Designated Nationals and Blocked Persons maintained by the Office of Foreign Asset Control (OFAC), which should be checked to ensure that potential customers do not appear on the same.

**Protecting the Confidentiality and Security of Customer Information**

Each employee is responsible for protecting the confidentiality and security of the customer information our Dealership collects and for using the information in accordance with our Privacy Policy. The following security procedures must be followed in order to protect our customer information:

1. Employees shall have access only to that customer information which is necessary to complete their designated responsibilities. Employees shall not access or provide any other unauthorized person access to customer information that is obtained during the course of employment. Employees must refer 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.

2. All paper and electronic records must be stored in secure locations to which only authorized employees 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.

3. 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. Passwords may not be posted near computers or shared any other person.

4. Employees that have access to the computer system and electronic records may not download any software or applications to our Dealership computers or open e-mail attachments from unknown sources. Employees must log off of any Internet, E-mail or other account when it is not in use.

5. Electronic records may not be downloaded to a disk or individual computer without explicit authorization from the Program Coordinator. If customer information is transmitted electronically over external networks, employees must encrypt the information at the time of transmittal.

6. All data must 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 must be shredded and stored in a designated secure area until an authorized disposal/recycling service picks it up.

7. Employees may not remove any customer information, whether contained on paper records or electronic records from the Dealership or disclose our security standards to any person who is not employed by us without authorization from the Program Coordinator.

8. Only that information which is necessary to complete a transaction initiated by the customer, is specifically authorized to be disclosed by the customer and/or is permitted to be disclosed by law shall be provided to service providers, marketers or any other parties. If you are unsure as to whether a specific disclosure is permitted, it is your responsibility to check with the Program Coordinator or your manager to verify that it is acceptable to release the information before doing so.

9. 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.

10. The Program Coordinator or appropriate manager should be notified 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.

11. When an employee ceases to be employed by the Dealership, he/she must turn in any keys that provide access to the Dealership and file cabinets, desks, and offices in the Dealership; passwords and security codes, if applicable, will be deleted.

**Disciplinary Action**

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

ADDENDUM

This Addendum modifies the _____("Agreement") entered into between _____("Dealer"), and _____("Company"). By executing this Addendum, 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 privacy and data protection laws, rules and regulations applicable now and in the future. Without limiting the generality of the preceding sentence, Dealer and Company agree that they will implement and maintain appropriate safeguards to protect customer information and that they will not use or disclose nonpublic customer 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. For purposes of this Addendum, the terms "nonpublic personal information" and "financial institution" shall have the meanings set forth in Section 509 of the Gramm-Leach-Bliley Act (P.L. 106-102) (15 U.S.C. Section 6809) and implementing regulations thereof. 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:**_____ |
| By:_____ | By:_____ |
| Its:_____ | Its:_____ |
| Date:_____ | Date:_____ |