

WHAT ARE THE RED FLAG RULES?

The Red Flag Rule is here to combat Identity Theft. Full compliance is required by NOVEMBER 1ST, 2008.

The cost of NON-COMPLIANCE specifically calls for civil penalties and fines. The act also allows for class action law suits.

To help consumers, the Federal Government has created rules which place requirements on companies that have a creditor relationship with a consumer. Included in that group are banks, savings & loans, credit unions, finance companies, debt collectors, health care companies, automobile dealers and any other company which maintains a creditor relationship with a consumer.

WHAT IS REQUIRED?

Dealers who finance even one car on their lot are subject to the new rules. Using any of the Social Security Number verification services is great and makes good business sense. That alone does NOT put in compliance. Each dealer must have a written Program that includes its own concerns and solutions.

THIS PROGRAM IS MANDATORY!!!!!!

IDENTITY THEFT RED FLAGS AND NOTICE
OF ADDRESS DISCREPANCY POLICY AND PROCEDURE

_____ (the "Dealership") hereby adopts the following Identity Theft Red Flags and Notice of Address Discrepancy Policy on this ____ day of August, 2008.

_____ (the "Program Coordinator") is hereby appointed as the Program Coordinator for this policy. The Program Coordinator will report to _____, the _____ of the Dealership. Should the Program Coordinator cease to be employed by the Dealership or is unable to perform her duties, _____ shall assume the responsibilities of the Program Coordinator until a new permanent Program Coordinator is appointed.

The Program Coordinator shall design, implement and maintain policies and procedures to identify "Red Flags" and notices of address discrepancy as defined the Fact Act of 2003 and the regulations implementing that Act and as identified in an audit of dealership practices and experience. These responsibilities include:

Identifying and assessing the risks of identity theft and discovery of address discrepancies in all areas of the Dealership;

Evaluating the effectiveness of current safeguards that have been implemented to control risks and to respond to situations in an appropriate fashion;

Designing and implementing appropriate policies and procedures;

Regularly monitoring and testing the policies and procedures for compliance with the applicable laws;

Regularly monitoring and testing the policies and procedures to determine their effectiveness in preventing identity theft;

Selecting appropriate service providers that can maintain safeguards to protect against identity theft;

Reviewing service provider contracts to ensure that each maintains appropriate procedures for identifying and responding to situations involving identity theft;

Regularly evaluating and modifying as necessary the Dealership's Policy in light of changes in the Dealership's operation, contracts and relationships and other matters that may impact the security or integrity of th Dealership's customer information and response to identity theft or a notice of address discrepancy;

Being 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 agency with her name, title and contact information.

If a possible identity theft or address discrepancy is identified, the Program Coordinator will send a report to the customer and, if necessary, and to the appropriate law enforcement agency. The report shall include: 1) The customer's name; 2) The date and type of transaction; and 3) The social security number, date of birth, address, and other personal identifying information provided by the customer.

All current employees and new employees as hired, 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;

Have access to customer information only for legitimate business reasons;

Receive training in Dealership's privacy policies, information security standards and this policy;

Sign and acknowledge their agreement to our Dealership's privacy policies, information security standards and this policy;

Protect the confidentiality and security of the customer information used by the Dealership;

Maintain the security of their computer passwords;

Refer requests for customer information to the Program Coordinator or appropriate manager other than requests received within the ordinary course of the Dealership's business;

Disclose to other persons or entities only that information which is necessary to complete a transaction initiated by the customer;

Notify the Program Coordinator or appropriate manager immediately of any attempts by unauthorized persons to obtain access to customer information

Notify the Program Coordinator or appropriate manager immediately of any password or customer information that has been subject to unauthorized access.

Any employee that fails to abide by this Procedure, whether intentional or unintentional, will be subject to appropriate disciplinary measures, up to and including termination of employment. If an employee is unsure as to whether a specific disclosure is permitted, the employee shall check with the Program Coordinator or appropriate manager to verify that it is acceptable to release the information before doing so.

When an employee ceases to be employed by the Dealership, they will be required to turn in any dealership keys in their possession. Password and security codes to which the employee had access will be deleted or changed. 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 will 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 is conflicting or cannot be verified, 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 relevant to the identity verification process will be retained by the Dealership for an appropriate retention period. Upon the expiration of that period, any such records will be disposed of in a proper manner.

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 to customer information only as necessary to complete their duties. Employees shall not access or allow others to access customer information other than as necessary to complete their duties. Employees must report to the Program Coordinator or appropriate manager, requests received by them for customer information that are outside the scope of the Dealership's ordinary business or their authorization.

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

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

Necessary backups of the computers and servers will be made at least daily. 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 will be updated and checked at regular intervals.

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 or destroyed and stored in a secure area until an authorized disposal/recycling service picks it up.

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

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

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

Selection and Oversight of Service Providers

In order to protect the Dealership's customer's information, 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 agreements 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 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 this policy is breached, the Program Coordinator will inform _____, the _____ of the Dealership. The Program Coordinator and _____ will take appropriate steps to notify counsel, service providers, customers, and the appropriate Law Enforcement Agency of any breach, damage or loss of information and the risks associated with the same and will immediately take measures to limit the effect of the breach, identify the reason for the breach and implement procedures to prevent further breaches.

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

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

As part of the audit program, Dealership personnel will be encouraged to advise the Program Coordinator of any newly identified risks to customers or to the safety of the Dealership regarding identity theft. To the extent that any newly identified risk 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 the Board of Directors regarding:

The effectiveness of the Program;

"Significant events" involving identity theft and management's response to any incident;

Recommendations for changes to this policy.

[DEALERSHIP LETTERHEAD]

[SERVICE PROVIDER ADDRESS]

Dear _____

In our effort to comply with the Fair and Accurate Credit Transactions Act of 2003 and the Federal Trade Commission's Implementing Regulation, we are requesting that all of the companies to which we provide nonpublic personal customer identity information acknowledge their agreement to maintain the confidentiality of and implement appropriate safeguards to protect such information in accordance with applicable laws. By signing below, you are agreeing that: 1) You will keep all nonpublic personal customer identity information provided by us about our customers confidential; 2) You will implement and maintain appropriate safeguards for the information you receive; 3) You will not disclose or use such information for any purpose other than as is reasonably necessary to fulfill the purpose for which such information was provided by us or as otherwise permitted by applicable law. In addition, you acknowledge that you have reviewed the relevant statutes and rules and will comply with each. In consideration of this, we will continue our business relationship with you and will provide you with information about our customers as necessary.

Please return this agreement to us by _____, 2008 at the above address. You may contact _____ at _____ if you have any questions.

Sincerely,

ACKNOWLEDGED

This _____ day of _____, 2008

Signed: _____

Print Name: _____

Title/Position: _____

ADDENDUM

This Addendum modifies any prior agreements (the "Agreement") entered into between the parties. 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.

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

Date: _____

Dealer: _____

Company: _____

By: _____

By: _____

Its: _____

Its: _____

[DEALERSHIP LETTERHEAD]

[SERVICE PROVIDER ADDRESS]

Dear _____ :

In our effort to comply with the Fair and Accurate Credit Transactions Act (Fact Act) of 2003 and the Federal Trade Commission's Implementing Regulations, we are requesting that all of the companies to which we may provide nonpublic personal customer identity information acknowledge their agreement to maintain the confidentiality of and implement appropriate safeguards to protect such information in accordance with applicable laws. By signing below, you are agreeing that you will keep all nonpublic personal customer identity information provided by us about our customers confidential, that you will implement and maintain appropriate safeguards for the information you receive, and that you will not disclose or use such information for any purpose other than as is reasonably necessary to fulfill the purpose for which such information was provided by us or as otherwise permitted by applicable law. In addition, you acknowledge that you have reviewed the relevant statute and rule and to comply with each. In consideration of this, we will continue our business relationship with you and will provide you with information about our customers as necessary.

Please return this agreement to us by _____, 2008 at the above address. You may contact (*name of contact person*) at (*telephone number*) if you have any questions.

Sincerely,

ACKNOWLEDGED

This _____ day of _____, 20

Signed:

Print Name:

Title/Position:

**EMPLOYEE ACKNOWLEDGMENT
REGARDING COMPLIANCE WITH THE FAIR
AND ACCURATE CREDIT TRANSACTIONS ACT**

The Fair and Accurate Credit Transactions Act requires motor vehicle dealerships, to: 1) Implement privacy policies and procedures to protect the information they collect; 2) Provide their customers with certain privacy notices; and, 3) Develop a written information security plan. As a condition of your employment with our Dealership, you agree to:

Read the Dealership's "Identity Theft Red Flags and Notice of Address Discrepancy Policy and Procedure" and familiarize yourself with the information contained therein.

Follow the Dealership's procedures for identifying identity theft red flags and notices of address discrepancies.

Follow the Dealership's procedures for responding to situations identifying real or potential identify theft of an address discrepancy in accordance with our Dealership "Identity Theft Red Flags and Notice of Address Discrepancy Policy and Procedure".

BY SIGNING BELOW, I ACKNOWLEDGE THAT I HAVE RECEIVED AND READ THE EMPLOYER'S IDENTIFY THEFT RED FLAGS AND NOTICES OF ADDRESS DISCREPANCIES POLICY AND PROCEDURES AND AGREE TO COMPLY WITH THE REQUIREMENTS SET FORTH THEREIN AS A CONDITION OF MY EMPLOYMENT. I FURTHER UNDERSTAND THAT FAILURE TO FOLLOW THE DEALERSHIP'S POLICIES AND PROCEDURES MAY RESULT IN DISCIPLINARY ACTION, UP TO AND INCLUDING THE TERMINATION OF MY EMPLOYMENT.

EMPLOYEE

DATE