GM DEALER COMPLIANCE
GLBA

GENERAL MOTORS DEALER INFORMATION TECHNOLOGIES

The Gramm-Leach-Bliley Act (GLBA) recognizes a financial institution as any business that engages in financial activities including insurance brokerage, data processing, and auto financing/leasing.

The GLBA's Safeguards Rule requires your dealership to develop a written information security plan that describes their process to protect customer information.

To be compliant with the Safeguards Rule, dealerships must:

- Designate one or more employees to coordinate an information security program
- 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
- Design and implement a safeguards program with regular monitoring and testing
- Select service providers that can contractually maintain appropriate safeguards
- Evaluate and adjust the program in light of relevant circumstances, including changes in a dealership's business or operations, or the results of security testing and monitoring

The Safeguards Rule also requires dealerships to assess and address the risks to customer information in all areas of their operation, including three areas of particular importance in terms of information security:

- Employee management and training
- Information systems
- Detecting and managing system failures

FTC Privacy Rule

The Privacy Rule applies to dealers who:

- Extend credit in connection with the purchase of a car
- Arrange the financing or leasing of a car
- Provide financial advice or counseling to individuals

Penalty for non-compliance:

Dealerships violating GLBA will be subject to a civil penalty of no more than $100,000 for each violation.

Security Requirements

- Ensure the security and confidentiality of customer data
- Protect against any reasonably anticipated threats or hazards to the security or integrity of customer data
- Protect against unauthorized access to, or use of, such data that would result in substantial harm or inconvenience to any customer

Encryption implementations should include:

- Encryption strength sufficient to protect the information from disclosure until such time as disclosure poses no material risk
- Effective key management practices
- Robust reliability
- Appropriate protection of the encrypted communication's endpoints

info@gmdit.com www.gmdit.com 866.526.8333