Here are the 9 steps that auto dealerships must follow under the FTC Safeguard Rule:

1. Designate an employee to coordinate your dealership's information security program. Auto dealers are required to implement and maintain reasonable safeguards to protect the security, confidentiality, and integrity of their customers' personal information. This includes the appointment of a designated employee who will be responsible for coordinating the dealership's Information Security Program.

The designated employee should have a thorough understanding of information security and data protection, as well as the ability to develop and implement policies and procedures to protect sensitive information. They should also have the ability to train and educate other employees on security best practices, and to monitor and enforce compliance with the Information Security Program.

To comply with Pennsylvania requirements, the dealership's Information Security Program should include the following elements: Identification and assessment of risks to the security, confidentiality, and integrity of personal information.

Implementation of reasonable administrative, physical, and technical safeguards to control these risks. Regular monitoring and testing of the effectiveness of the safeguards.

Regular training for employees to ensure their understanding of the Information Security Program and their obligations under it.

A plan for responding to security incidents and conducting investigations. Regular review and update of the Information Security Program to reflect changes in technology, the dealership's business operations, and the threat environment.

By implementing and maintaining these elements, auto dealers can meet their legal obligations to protect their customers' personal information and ensure the security of their dealership.

2. Identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks. How do auto dealers conduct an assessment to determine foreseeable risks and threats – internal and external – to the security, confidentiality, and integrity of customer information in order to comply with the FTC Safeguard Rule.

Auto dealers can conduct an assessment to determine foreseeable risks and threats to customer information by following these steps:

Identify the information they collect and store. Identify internal and external risks to the security, confidentiality, and integrity of the information. Evaluate the sufficiency of their current safeguards and procedures. Design and implement a written information security program (WISP) to address identified risks and safeguard customer information.

Monitor and regularly reassess the effectiveness of their WISP and adjust as necessary. To comply with the FTC Safeguard Rule, auto dealers must also provide employee training, oversee service providers, and develop procedures to respond to security incidents.

3. Design and implement information safeguards to control the identified risks, including measures to:

• Ensure the security and confidentiality of customer information

• Protect against any anticipated threats or hazards to the security or integrity of such information

• Protect against unauthorized access to or use of customer information that could result in substantial harm or inconvenience to any customer. Conduct a periodic risk assessment to identify and prioritize potential risks to customer information.

Implement access controls, including periodic reviews of who has access to customer information and why.

Conduct a periodic inventory of data and maintain an accurate list of all systems, devices, platforms, and personnel.

Encrypt customer information both on the company's system and when it's in transit.

Assess the security of any apps used to store, access, or transmit customer information.

Implement multi-factor authentication for anyone accessing customer information on the system.

Securely dispose of customer information no later than two years after the most recent use.

Anticipate and evaluate changes to the information system or network and build change management into the information security program.

Maintain a log of authorized users' activity and monitor for unauthorized access to customer information.

4. Regularly monitor and test the effectiveness of the safeguards' key controls, systems, and procedures. Auto dealers can regularly monitor and test the effectiveness of their safeguards by: Conducting regular testing of procedures for detecting actual and attempted attacks, including penetration testing and vulnerability assessments.

Implementing continuous monitoring of the information system to identify and respond to security incidents. Conducting annual penetration testing and vulnerability assessments, including system-wide scans every six months to test for known security vulnerabilities.

Testing the safeguards whenever there are material changes to the dealership's operations or business arrangements that may impact the information security program.

Monitoring and reviewing audit logs to detect potential security incidents and breaches.

Implementing procedures for promptly responding to security incidents, including investigating and remediating any identified vulnerabilities or weaknesses in the information security program.

Providing periodic employee training and security awareness programs to reinforce the importance of information security and the safeguarding of customer information.

5. Evaluate and adjust your information security program in light of relevant circumstances, including changes in your dealership's business or operations, or the results of security testing and monitoring.

Conduct regular risk assessments to identify new and emerging risks to the security, confidentiality, and integrity of customer information. Evaluate your information security program periodically to ensure that it remains effective in addressing the risks identified through your risk assessments. Keep your employees and service providers informed of changes to your information security program and provide them with regular training and awareness updates. Stay current with new and emerging threats and countermeasures by monitoring industry publications, attending conferences and seminars, and engaging with other information security professionals. Be prepared to modify your information security program in response to changes in operations, personnel, and other circumstances that may have a material impact on the program. Review and update your information security program on a regular basis to ensure that it remains current and effective in protecting customer information.

6. Train your employees on the importance of information security and how to follow the dealership's information security policies and procedures. To comply with the FTC Safeguard Rule, auto dealers must train their staff in information security to help prevent security incidents and protect customer information. The following steps can be taken:

Provide regular security awareness training to all employees, including those with non-technical roles, to educate them about their role in safeguarding customer information and to identify and respond to security incidents.

Schedule regular refreshers to ensure employees are up-to-date on the latest threats and countermeasures.

Provide specialized training for employees, affiliates, or service providers with hands-on responsibility for carrying out the dealership's information security program. Verify that all employees have completed required training and can demonstrate an understanding of the safeguards in place to protect customer information.

Ensure that employees, affiliates, or service providers understand the importance of maintaining the confidentiality and security of customer information, and the consequences of failing to comply with the dealership's information security program.

Encourage reporting of security incidents or suspicious activity and establish procedures for employees to follow in the event of a security incident.

7. Select service providers that are capable of maintaining appropriate safeguards, and require those safeguards by contract. Include specific security requirements in your contracts with service providers, including details about the types of information they will have access to, how they will protect it, and how they will notify you of any security incidents.

Require service providers to certify that they have implemented appropriate safeguards to protect customer information.

Establish ongoing monitoring of service providers to ensure that they are meeting their security obligations under your contract, including regular security assessments and review of their security practices.

Ensure that service providers are aware of their responsibilities under the FTC Safeguard Rule and are taking appropriate steps to comply.

Review your contracts with service providers periodically to ensure that they remain appropriate and that your service providers are continuing to meet your security expectations.

8. Establish procedures for periodically obtaining written assurances from your service providers that they have implemented and are maintaining appropriate information security practices. The Federal Trade Commission (FTC) Auto dealer Safeguards provide guidelines for auto dealers to protect consumers' personal and financial information. The requirement for obtaining written assurances from service providers is an important step in ensuring the security of customer information.

By obtaining written assurances from service providers, auto dealers can ensure that their service providers have implemented appropriate information security practices, such as encryption, firewalls, and access controls. This also allows auto dealers to verify that their service providers are following industry standards and regulations related to data security.

It is important for auto dealers to establish a regular schedule for obtaining these written assurances to ensure that their service providers are maintaining appropriate information security practices over time. This can be done through regular audits, security assessments, or other means, and it should be documented as part of the auto dealer's overall information security program.

Overall, the FTC Auto dealer Safeguards are designed to help protect consumers' personal and financial information and to promote responsible data practices in the auto industry. By following these guidelines and regularly verifying the security practices of their service providers, auto dealers can help ensure the protection of their customers' sensitive information.

9. Evaluate and adjust the information security program whenever there is a material change in your dealership's operations or business arrangement, including material changes to the services provided by service providers. The Federal Trade Commission's Safeguard Rules for auto dealerships require that the dealership's information security program be evaluated and adjusted whenever there is a significant change in the dealership's operations or business arrangements. This includes changes to the services provided by third-party service providers. The purpose of this requirement is to ensure that the

dealership's information security program remains effective and relevant in the face of changing circumstances.

By regularly reviewing and updating their information security program, auto dealerships can ensure that they are protecting sensitive customer information, such as personal and financial data, against unauthorized access or theft. This is crucial in maintaining the trust and confidence of customers and helping to prevent costly data breaches.

Overall, the FTC's Safeguard Rules serve as guidelines for businesses to follow in order to protect the privacy and security of their customers' sensitive information. Auto dealerships should take these rules seriously and regularly evaluate and adjust their information security programs to ensure they are meeting the latest standards for data protection.