Data Security and Privacy Compliance
Risk Assessment Questionnaire

What is the purpose of this tool?
The purpose of this tool is to help simplify and standardize dealership and vendor compliance with the federal Gramm-Leach-Bliley Act (GLBA) Safeguards Rules (hereinafter referred to as the "Rule") requirement to have dealers periodically assess their service providers for the adequacy of their physical, administrative, and technical information safeguards. The tool is meant to be completed by "Service Providers" to demonstrate their ability to adhere to privacy and cybersecurity standards set forth in the Rule. Under the Rule, a "Service Provider" is any vendor that retains, receives, accesses, collects, uses, or discloses customer personal information from the dealership(s). Dealers can also use the tool to proactively send it to their Service Providers for completion.

Why do Service Providers need to complete this?
Under the Rule, dealers are required to periodically assess their Service Providers' current data security and privacy policies, processes, and practices. In response to a comment from the National Automobile Dealers Association (NADA), the Federal Trade Commission (FTC) has advised that dealers should not continue to do business with Service Providers who are unable or unwilling to complete such assessments. Therefore, Service Providers can complete this tool to help avoid any interruptions in business or allegations of non-compliance.

Cybersecurity Framework Mapping
For your convenience, each of the metrics listed in the tool has been mapped to the closest corresponding section of certain popular cybersecurity frameworks, such as NIST, ISO 27001, CIS, SOC2, and PCI.

Risk Assessment Questionnaire

Risk Assessment & Treatment

Undertake regular information risk management for the service through consistent processes under a structured, documented methodology.

Q: Do you have a written information security program? [GLBA]

Q: Do you manage access and permissions to personal information (whether stored physically or electronically) using role-based, least-access, or need-to-know principles? [GLBA]

Q: Do you perform physical, administrative, and electronic risk assessments relating to information safeguards at least annually? [GLBA]

Q: Do you have a documented process (and provide mechanisms for) the secure destruction and disposal of documents containing customer personal information after the expiration of a legitimate business or legal need? [GLBA]

Q: Do you perform penetration tests at least annually? [GLBA]

Q: Do you perform vulnerability scans or assessments at least biannually? [GLBA]

Third Party Services Compliance

Suppliers, vendors, and others you may engage services of, and their compliance in these safeguard rules in your business.

Q: Do you require that each of your service providers and sub-processors sign a data processing agreement that complies with applicable state and federal data privacy laws? [GLBA]

Asset Management

Q: Do you have endpoint detection and response (EDR) software installed on all endpoint devices that is continuously monitored and managed? [STAR Recommendation]

Q: Do you regularly update and patch operating systems and applicable third-party software and test your network to ensure that such updates and patches have been successfully installed on all applicable devices? [STAR Recommendation]

Q: Do you require the use of multi-factor authentication (MFA) to login to all on-premises workstations, servers, and systems containing nonpublic personal information? [GLBA]

Q: Do you support and require the use of multi-factor authentication (MFA) on your own third-party cloud-based applications containing nonpublic personal information? [GLBA]

Q: Do you require the use of multi-factor authentication (MFA) for all company email accounts and identity services? [STAR Recommendation]

Data Security and Privacy

Q: Do you train your engineers in secure coding practices? [STAR Recommendation]

Q: Do you follow platform and OS guidelines for security? [STAR Recommendation]

Q: Do you use anonymized data in test systems? [STAR Recommendation]

Q: Do you verify privacy and security features work as intended? [STAR Recommendation]

Q: Do you conduct (1) social engineering and phishing simulations and (2) security awareness training for applicable employees at least annually? [GLBA]

Q: Do you require the use of complex and unique passwords (alpha-numeric and non-dictionary words) for all systems containing customer personal information, including both internal and client-facing applications? [STAR Recommendation]

Q: Do you use properly configured and industry-tested methods of encryption to keep customer personal information secure in transit and at rest? [GLBA]

Business Continuity

Q: Do you perform automated backups of sensitive data or critical enterprise assets that are either stored offline or on segregated systems? [STAR Recommendation]

Q: Do you have a cybersecurity insurance policy that covers data breaches affecting customer personal information that you collect, receive, store, or process on behalf of dealers and other clients? [STAR Recommendation]

Q: Do you configure all workstations and devices with automatic locking after a defined period of inactivity? [STAR Recommendation]

Q: Do you use application allow-listing to restrict employees' ability to install and run unauthorized software? [STAR Recommendation]

Q: Do you protect against brute-force attacks by suspending or disabling user credentials after a certain number of unsuccessful login attempts? [STAR Recommendation]