10 STEPS DEALERS NEED TO TAKE TO PROTECT "DEALER DATA"

1. Conduct an audit of access to your DMS and other dealer systems

Know and understand who is in your systems and what they have access to - both employees and third parties. Review external access to all of your systems and databases (DMS, CRM, websites, *etc*.). Work with your vendors and don't forget non-DMS databases or data access points (*e.g*., online credit applications). Review password authorization policies to ensure that internal and external access is limited appropriately. If another third party is gathering data on behalf of your service provider, you *must understand and limit that access just as you limit access by your service providers.*

2. Determine and limit scope of access / control passwords

Delete all outdated or unauthorized access and require all third party service providers with legitimate access to provide written list of data they have access to as well as a listing of all data fields they are "taking." Ensure that you understand and appropriately limit the scope of access that all your authorized service providers have. For example, if a service provider is providing services related to your parts department, it should not have access to sales data. Document all access and any changes to access. Establish protocols for adding or expanding data access. Work with your DMS provider to ensure proper controls and reporting.

Centralize and control authority to grant password access and scope of access to dealer systems. Work with your DMS provider to monitor and audit. Require regular changes to passwords, and require employees to use "stronger" passwords for any access to sensitive data.

3. Review all contracts and *ensure required GLB language is included*

GLB requires that you include provisions in your service provider contracts that (a) prohibit the service provider from accessing data beyond what they need or from using that data for any purpose other than providing you with the service, and (b) require the service provider to take steps to safeguard customer data they obtain from you. You must understand what data your third party service providers need and why. To do this, you must understand the service provided and legitimate reasons for the scope of data accessed. YOU MUST limit this via contract with your service providers *as well as with anyone who accesses or obtains data on their behalf*. Take steps to audit service providers regularly. Seek regular written confirmation, run internal reports, hold your service providers accountable, and document your processes!

Consider the use of the NADA *Service Provider Data Access Addendum.* This document is intended to be used by dealers to amend their current service provider agreements to ensure that the required contractual provisions are included. Consult your counsel.

4. Consider implementing a strict data "push" system for sharing data

This means that you need to understand what data a service provider needs to provide the service, gather it internally from your systems (or through a vendor), and send it to the appropriate service providers in a secure manner. You would no longer allow vendors to access your systems directly for any reason. This approach allows you to have control over what data is shared, prevents concerns regarding the scope of access, and provides a documented audit trail of all data you have shared. Note that it is possible that a push system could affect the functionality of some services. However, carefully

consider claims by vendors that they "need" "real-time" access. In many cases, regularly "pushed" data will be more than adequate.

5. Understand and control remote access issues

Mobile devices raise tremendous data access and data breach concerns. You should take steps to limit remote access and control the devices that provide access. Work with your counsel and DMS and other vendors to address the policy, security, and business implications of mobile device access. Consider the implications of remote access from employees "home" computers. Enact policies to control data access, copying, and sharing.

6. Understand data flow to your manufacturer(s)

You may not share certain protected data – even with your manufacturer – unless an exception to the Privacy Rule applies. This is a complicated area that depends highly on the facts and circumstances. If your manufacturer seeks to obtain NPI, get written confirmation that it is pursuant to an exception to the Privacy Rule.

7. Understand "P2P" ("Peer-to-Peer") networks and enact a "P2P" policy

Have a policy, train your employees, and consider prohibiting access to P2P sites. Go here for more information: http://business.ftc.gov/documents/bus46-peer-peer-file-sharing-guide-business.

8. Understand data and privacy implications of your social media efforts

Do you gather any customer information via social media? What is your involvement with customer comments/dealership reviews? Do you engage the services of a "reputation management" vendor? Do you understand *exactly* what services they are providing, what they have access to, and why?

9. Confirm that your Privacy Notice is accurate!

Use the Model Privacy Notice form, and review "*A Dealer Guide to the FTC Privacy Rule and Model Privacy Notice*" at www.nadauniversity.com. Ensure that you are properly using the model notice form. If you share customer information with service providers, you must properly disclose that on your privacy notice.

10. Consider additional steps to segregate and track data

For example, consider segregating your data to further protect the most sensitive and valuable data - by store; by manufacturer; and by separating "sensitive" data from "non-sensitive." You can segregate the data physically (different servers/systems) or by password. The more you segregate the data, the more control you have over access to that data – both internal and external.

Another step to consider is the use of "dummy" or false customers in your databases with a physical and email address you can monitor. Once inserted, you can then test what, if any, marketing information comes to that "customer." This can provide good insight into who may be accessing your data without your knowledge.