Kentucky Automobile Dealers Association
The Voice of Automobile Dealers in Kentucky

STOLL KEENON OGDEN PLLC

June 10, 2022

Winter is Coming Part 4: Mandatory Safeguards and an Acronym You Never Knew You Needed

DISCLAIMER: The information in this document may change over time with new information and developments. All content and materials are for general information purposes only. It does not provide, and is not intended to constitute, legal advice. Important: As necessary, dealers should consult an attorney familiar with dealership operations, Federal, State and/or local laws at issue.

This article is the fourth in a series of materials to help your dealership with the appropriate planning and implementation of the necessary policies and procedures required by the FTC's amended Safeguards Rule, the vast majority of which require dealer compliance by December 9, 2022.

Part three of our series described the need to conduct a risk assessment. Once that is completed, the next step is to implement specific safeguards to protect consumer data. The amended Safeguards Rule includes very specific measures to be included as part of your information security program.

Mandatory Safeguards

1. Access Controls: Dealerships must implement controls limiting access to consumer information, regardless of whether than information is stored electronically or via paper copies. For electronic information, this means password protecting files containing customer information. For information physically stored on site, this could mean using locks or restricted key card access. Of course, personnel should be limited to accessing such information only when it is necessary for work functions.

2. System Inventory: This inventory, while limited to only those systems that contain consumer data, can be an overwhelming concept, because it requires identification of all data, personnel, devices, systems, and facilities that your business utilizes. In addition to your on-site computers or information technology, this inventory can include: your websites, lead generators, OEM sites, appointment scheduling software, personal computers of employees who may work from home, mobile phones of sales personnel which contain customer names and phone numbers, as well as third parties that may store or process your data.

3. Encryption: The FTC defines encryption as, "the transformation of data into

a form that results in a low probability of assigning meaning without the use of a protective process or key, consistent with current cryptographic standards and accompanied by appropriate safeguards for cryptographic key material." Translated, this just means that information is encoded to render it unreadable without the encryption key or password. Data should be encrypted both when it is shared and when it is stored within your internal systems. While this can sound complicated, there are low-cost encryption options available. The FTC also included an exception for this requirement where your Qualified Individual determines that encryption of certain customer information is not feasible.

4. Secure Development Practices: Most dealers do not develop their own in-house software applications, so application of this requirement is to the evaluation of third-party software by dealerships to ensure that it is secure. While the FTC rule is far from clear, the comments to the rule indicate that you are not required to undertake any specialized review of vendor infrastructure or coding. Where software has been tested by third parties, as we expect will be the case for most programming you utilize, a review of the results is sufficient.

5. Multi-factor Authentication (MFA): This requirement will be discussed in detail below, but the amended Safeguards Rule requires you to implement multi-factor authentication (or reasonably equivalent controls) whenever any individual - whether employee, customer or otherwise - accesses an information system that contains customer information.

6. Disposal Procedures: While the rule allows customer information to be stored for as long as it is necessary for business operations or a legitimate business person, once it is no longer needed it should be securely destroyed within two years. This does not mean that you must destroy information two years after a sale. In fact, you probably should not, as banking and other regulatory requirements likely require a longer retention period. Instead, data should be destroyed by a reputable vendor or shredded within two years after you no longer have any business reason to retain it.

7. Change Management Procedures: While this portion of the amended Safeguards Rule does not require any specific security procedure, it does require that dealers have a procedure to evaluate the security of devices, networks, or programs added to their information system, as well as the impact on security of removing any device, network, or program.

8. Monitoring Unauthorized Use: Your dealership should have policies and procedures in place that will detect unauthorized access of customer information by authorized users, as well as logging personnel activity when accessing customer information. If there is a security breach, this will assist management in determining what information was accessed.

The Keys to Multi-factor Authentication (MFA):

MFA is not a Master of Fine Arts to the FTC. You are probably familiar with multi-factor authentication if you have accessed medical information online in the last couple of years. While valuable for security purposes, MFA is often criticized for creating delay and disruption for users. The FTC defines "multi-factor authentication" as authentication that uses two of the following: 1. Knowledge factors, such as a password; 2. Possession factors, such as a token or passcode; or 3. Inherence factors, such as biometric features. The most common form of multi-factor authentication is an employee's use of a

password (knowledge) combined with a passcode sent to a mobile device (possession).

One option for limiting the disruption or delay that MFA can cause is segmenting your network or information system to isolate consumer information. This way, employees can perform tasks that do not require customer data do not need to use MFA to access necessary applications. Segmenting can also create a way to limit access to consumer information to only those personnel who need it. Implementing MFA is likely to be a burden, at least in the beginning, but it is the most effective method for securing your data of all the required safeguards, so it is worth the cost in both time and money to comply with this requirement.

Once again, the amended Safeguards Rule allows dealerships to appoint third-party vendors to assist with these new requirements and as a vetted KADA Preferred Partner, we recommend the resources and services that ComplyAuto offers. You can find their contact information below.

For further information, please contact:

Sarah Bishop: (502) 875-6245; sarah.bishop@skofirm.com
Ron Smith: (317) 822-6787; ron.smith@skofirm.com

ComplyAuto contact:
Hao Nguyen: (510) 676-8579; hao@complyauto.com