Kentucky Automobile Dealers Association
The Voice of Automobile Dealers in Kentucky

STOLL KEENON OGDEN PLLC

June 27, 2022

Winter is Coming Part 5: Testing the System

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 fifth 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.

Establishing your information security needs and implementing appropriate controls is just the beginning of FTC compliance under the new safeguards rule. The revised rule not only requires regular testing of your security program, but it specifies the frequency and type of the required testing.

Depending on specific circumstances, you may be required to conduct continuous monitoring or a combination of penetration testing and vulnerability assessments. Continuous monitoring is designed to detect changes in the information system that might create vulnerabilities on an ongoing basis. Penetration testinginvolves an attempt to defeat security measures and access databases or controls from outside the organization. If you are not performing continuous monitoring, you must perform penetration testing on an annual basis. Vulnerability assessments include systemic scans of information systems to identify publicly identifiably security vulnerabilities. If you are not performing continuous monitoring, you must perform vulnerability assessments at least every six months, as well as any time there are material changes to your operations and whenever you are aware of circumstances creating a risk to your security program.

NADA recommends a mix of monitoring and testing. Specifically, NADA suggests a patch management system that provides vulnerability scanning at least monthly, if not weekly, along with annual penetration testing. Your information technology specialists, whether in-house or an outside vendor, should be able to walk you through these options. And of course, with any outside vendor that has access to your data, you are ultimately responsible for taking steps to ensure that they use adequate security measures to protect

consumer information.

Once again, 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

Visit our website:www.kyada.com

Follow KADA on Facebook