The Amended FTC Safeguards: Moving Toward Compliance

The Federal Trade Commission's Amended Safeguards Rule has been the subject of multiple articles, webcasts, seminars and more, and with good reason. The amendments to the Safeguards Rule pose significant hurdles for dealers, and the deadline for compliance— December 9, 2022— will be here before you know it. While most dealers have begun taking the necessary steps to be fully compliant on time, a reminder of the appropriate steps is in order for everyone. While this is not a comprehensive discussion of the Amended Safeguards, it should assist you in evaluating your progress toward full compliance.

Step One: Designate a Qualified Individual

Your "Qualified Individual" will be the primary point of contact for oversight and implementation of your information security program. While the Qualified Individual is not required to have any specific information technology education or training, him or her should be a senior member of your staff and should be knowledgeable about your current information security measures. You are permitted to designate a contractor to serve as your Qualified Individual, but that will not shield your business from ultimate responsibility if your compliance is deficient or if there is a security incident.

Step 2: Assess Your Risk

Under the Amended Safeguards, Risk Assessments must be conducted "periodically," which is not defined therein, but is generally interpreted to mean at least annually if not more frequently. A Risk Assessment is a written document that evaluates security risks to customer information maintained by your dealership and measures the adequacy of your current safeguards. Ultimately, your security program will be based upon the vulnerabilities identified through the Risk Assessment.

Step 3: Implement Mandatory Safeguards

The mandatory safeguards required by the FTC can be daunting, and include: controlling internal and external access to customer data; establishing an inventory of all locations, physical or electronic, of customer data; using encryption to protect data; establishing a multifactor identification program; ensuring development practices are secure; disposing of data in a secure and appropriate manner; developing procedures to maintain security when there are changes to your system; and monitoring and logging user activity. Most dealerships will need some outside assistance with this undertaking but should be cautious that your service providers must also maintain adequate information security practices.

Step 4: Test Your Controls

Once you have implemented the mandatory safeguards, you are required to test their efficiency. You are required to use either continuous monitoring to test your security program or to perform annual periodic penetration and vulnerability assessments. Penetration testing involves attempting to access your information system from outside that system and would need to be performed annually if you do not elect to use continuous monitoring. A vulnerability assessment involves scans of your information systems to identify known security risks and is required every six months if you do not use continuous monitoring.

Step 5: Develop Personnel Policies

This portion of the Amended Safeguards requires security awareness training to all staff and some level of specified training for any personnel directly involved with your information systems. You are likewise required to use security training that is up to date with respect to current security practices and risks.

Step 6: Oversee Your Vendors

You are responsible for ensuring that any vendors with access to your customer data maintain adequate safeguards to protect the security of that data. Dealers cannot simply rely on contractual assurances from their vendors (although they should obtain those assurances), but must engage in some level of due diligence to make sure that your service providers have a record of safe practices. Similarly, you should review these practices on occasion. It may be advisable to have consent to a third-party security review as part of your vendor contract.

Step 7: Prepare an Incident Response Plan

An incident response plan is a written document that you must prepare to provide a guide for the steps your business will take in the event of a security event — defined as an event resulting in unauthorized access to, or disruption or misuse of an information system or customer information stored in physical form. Importantly, a security event can occur even if there is no risk of resulting consumer harm. Thus, even unsuccessful attacks to your system could create a security event. Your incident response plan should include not only the steps you will take to respond to the event, but a description of lines of decision-making authority and a description of internal and external communications that will be used following a security event.

Step 8: Prepare an Annual Report

Another required written document, an annual report should discuss not only the overall status of your information security program, but also an overview

of the results of any risk assessments, steps taken to comply with the Safeguards, arrangements made with vendors or service providers, as well as any actual or threatened security events. The Annual Report should be made by your Qualified Individual on an annual basis to the board of directors or, in the absence of a board of directors, to a senior member or company official with authority over the information security program.

These requirements can be overwhelming, especially if you have not already begun to implement them. If your dealership needs assistance in compliance, there are vendors available to support your development of the required procedures, such as KADA's Preferred Partner, ComplyAuto.

For questions or further information, please contact your Stoll Keenon Ogden Automotive Dealership Services team:

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