FTC Safeguards Rule Basics Checklist

As a marine dealer operating in the United States, you must demonstrate an ongoing good-faith effort with federal rules and regulations to be compliant. Many rules, such as the FTC Safeguards Rule, may require that you adapt your processes to ensure compliance. Certain provisions of the current FTC Safeguards went into effect on January 10, 2022, while other provisions take effect on June 9, 2023.

While this is not an all-inclusive list, here are 9 critical steps your dealership must take in order to make a good-faith effort to comply with the updated FTC Safeguards Rule:

Check	Action Items
	Designate a "qualified individual" that will implement, oversee, and enforce your information security program (ISP), and qualified information security/technology personnel to help the qualified individual oversee and implement the ISP.
	Conduct periodic written risk assessments identifying internal and external risks to customer information. This requires knowing where physical and electronic customer information resides, who has access, and on which devices.
	Create a written information security program based upon the risk assessment that identifies the administrative, technical, and physical safeguards.
	Provide and document security awareness training and testing to all employees that may have access to customer information. Testing should include simulated phishing attacks.
	Select service providers capable of appropriately safeguarding customer information, periodically assess them, and contractually require them to appropriately safeguard customer information.
	Enable physical and technical access controls, such as creating secure document areas with limited access, using locked filing cabinets, establishing clean-desk and clean-screen policies, establishing logging of systems (electronic and physical) for audit trails, establishing acceptable use policies for electronic hardware and software, establishing change-management procedures, and establishing appropriate data and document retention and destruction policies.
	Ensure all information security systems have encryption (in-transit and at-rest), multi-factor authentication enabled, and are continuously monitored for attacks and intrusions into information systems (absent effective continuous monitoring, annual penetration testing and vulnerability scanning every six months may be conducted).
	Establish an Incident Response Plan (IRP) identifying the actions that will be taken if a security event/violation would occur. The IRP will include methods for detection, response, notification, remediation, and improvement to the ISP.
	Provide a written status report to the Board of Directors or equivalent governing body/executive(s) from the qualified individual identifying overall compliance and material matters, including risks assessed, risk management and control decisions, service provider arrangements, results of testing, security events/violations and management's responses, and recommended changes to the ISP.

These are key ingredients your business must include in its efforts to achieve compliance in order to protect your business, employees and customers. However, there is more to know, understand, and do to demonstrate your team's compliance. Learn more at mraa.com/safeguardsrule.

MRAA connects you to trusted experts and the resources they have developed, including the following:

- Is Your Dealership Ready for Training Curriculum Required Under New FTC Safeguards Rule? by Ken Hill, 700Credit, an MRAA Education Champion
- Compliance Guidance for the Revised FTC Safeguards Rule by Adam Crowell, President and General Counsel of ComplyNet

700Credit CREDIT | COMPLIANCE | SOFT PULLS

MRAA MARINE RETAILERS ASSOCIATION OF THE AMERICAS

COMPLYNET