



Comments from Andrew MacKay, Executive Director of the NV Franchised Auto Dealers Association Regarding Senate Bill 44

First, I would like to begin by putting it on the record that Nevada's franchised automobile dealers work diligently everyday to ensure that our customers' personal information and data is protected at all costs. We spend tens of thousands of dollars every month working with cybersecurity experts to ensure our systems are robust, up-to-date, and designed in such a way as prevent cybercriminals from accessing all types of information. For them, they only need to be right once. For us, we need to be right 100% of the time.

Why are we opposed to SB 44? Simply put the provisions of the bill are duplicative of current federal law, including providing notification to the Federal Trade Commission (FTC) of an unauthorized acquisition of unencrypted information of 500 or more customers pursuant to the FTC's Safeguards Rule. It is important to note that these incident reports become part of a publicly accessible database which is maintained by the FTC. As a result, any information the state seeks to obtain under SB 44 is already readily available with a couple clicks of a computer mouse.

Before I get into specifics, I think it's a somewhat important to provide a bit of history on the Safeguards Rule which our member dealers have been dealing with for years and to emphasize that penalties for non-compliance are steep, exceeding more than **\$46,000 per violation**. In addition, violating the rule could result in a claim under the Unfair Deceptive Acts and Practices (UDAP) laws of the state resulting in enforcement action from the Nevada Attorney General's office. As a result, any concern the state may have with respect to a lack of penalties pertaining to non-compliance are simply unfounded.

The FTC Safeguards Rule was initially issued in 2002 under the Gramm-Leach-Bliley Act (GLBA) and took effect on May 23, 2003. Fast forward 18 years, on December 9, 2021, after several years of notice and comments, public hearings and debate, the FTC officially published revisions to the Safeguards Rule requiring dealerships to revise their information security programs and implement new compliance measures.

Due to the complexity of the revised rule, the tremendous preparatory costs (NV dealers spent millions of dollars just on this task), and various steps needed to comply with the rule, the FTC extended the effective dates of several provisions of the rule three different times, with the entire rule ultimately being in full force and effect in May of 2024.

What are some the requirements of the current FTC Safeguards Rule? Here is a small sampling:

- Conduct routine assessments on information security which evaluate both internal and external security risk.
- Implement mandatory safeguards to control risk such as the creation of a written information security system, severely limiting access to customer data, and extensively encrypting all data.
- Routinely test and audit the effectiveness of the company's safeguard key controls, systems, and procedures. As to information systems, the requires either continuous monitoring or a combination of both penetration testing and vulnerability assessments.

While I could certainly go on about the FTC's Safeguards Rule and the many things our vendor partners and we (NFADA) do to assist our members with compliance - including the creation of a *59-page Driven Guide* by the National Automobile Dealers Association – I think the record clearly demonstrates the duplicative nature of SB 44 is unnecessarily burdensome for Nevada's vehicle dealers and we strongly believe we should be exempt from the provisions of Senate Bill 44.