FTC Hosts Workshop to Examine Proposed Changes to Its Safeguards Rule

August 31st, 2020

Nora R. Udell

The Federal Trade Commission held a virtual workshop on July 13, 2020, to examine its proposed amendments to the Safeguards Rule. The Safeguards Rule, promulgated under the Gramm-Leach-Bliley Act, requires financial institutions, including auto dealers, to develop, implement, and maintain a comprehensive information security program. The rule hasn't been updated since it originally became effective in 2003, and the FTC is freshening it up! If you want to submit comments about the proposed amendments, you have until August 12, 2020, to do so.

The workshop examined many of the FTC's proposed changes, including that financial institutions must encrypt customer data, use multifactor authentication to access customer data, and have a single qualified individual, called the Chief Information Security Officer, to be responsible for overseeing, implementing, and enforcing the information security program. The amendments further require institutions to perform a written risk assessment, conduct continuous monitoring or annual penetration testing and biannual vulnerability assessments, prepare a written incident response plan, and prepare an annual written report by the CISO.

A hallmark of the original Safeguards Rule is its flexibility. Since 2003, the rule has provided general guidance for an information security program without being overly prescriptive about what it must include. The FTC explained in its 2019 proposed amendments, and reiterated at the recent workshop, that it wants to retain that flexibility while also providing more detailed guidance about what an appropriate information security program entails.

Cost and scalability for smaller businesses were the topic of many comments the FTC received and much of the all-day workshop. Lee Waters, IT Manager at McCloskey Motors in Colorado Springs, who has experience implementing the current Safeguards Rule, spoke on the "Information Security Programs and Smaller Businesses" panel. He detailed the costs that dealerships could expect in becoming compliant with the proposed changes to the rule. For example, he reviewed the potential costs of hiring an in-house CISO or outsourcing that role, implementing multifactor authentication and penetration testing, and updates to physical security.

The panelists discussed methods to mitigate these costs, which, I'm sure you can imagine, were well into 6-figure territory. For example, the biggest cost likely is hiring a CISO. Waters discussed using a current IT employee to fill the CISO role, with assistance from an outside service provider or vendor. For dealerships without an IT staff, a service provider or vendor may be the only option. In general, three models for the CISO role were discussed: (1) an in-house model where an existing

member of the team, with proper training, acts as the CISO; (2) an outsource model where the company engages a service provider to manage the program; and (3) a hybrid approach where an employee manages the program and outsources activities as needed for expertise.

A little good news is that the cost to implement encryption and multifactor authentication will be more manageable. Vendor products are available for encryption, and some you already use, like Microsoft products, may have encryption capabilities. Some companies offer free multifactor authentication for up to a certain number of end-users.

A little more good news is that the proposed changes would exempt certain small businesses from most of the rule's requirements. Financial institutions exempt from most of the Safeguards Rule requirements are those that maintain customer information on fewer than 5,000 consumers.