Legal Musings: Keep Privacy and Data Security on Your Radar

May 4th, 2021 | and Patricia E.M. Covington

This article was originally published in the May 2021 issue of *Used Car Dealer Magazine*.

Privacy and data security. If you don't have those issues on your radar, you should. Dealers have always had data privacy and safeguarding responsibilities. Nothing new here. But a change is coming. The basic privacy and data security concepts and requirements we've grown accustomed to are expanding – actually, transforming – into fundamental and robust consumer privacy rights. Data security is also evolving from a general set of principle-based requirements to more obligations.

The Virginia legislature recently enacted a comprehensive consumer data privacy law called the Virginia Consumer Data Protection Act. The VCDPA follows the California Consumer Privacy Act – the nation's first comprehensive consumer data privacy law, which became effective last year. Californians were not content with the CCPA, so in November they passed the Consumer Privacy Rights Act through a ballot initiative. The new law, which becomes effective Jan. 1, 2023, beefed up the state's already comprehensive privacy and data requirements. Other states are currently considering similar legislation, including Washington, Texas, Utah, Arizona, New Mexico, Oklahoma, Alabama, Florida, South Carolina, Kentucky, Illinois, Minnesota, Nebraska, North Dakota, Pennsylvania, New Jersey, Maryland, New York, Connecticut, Rhode Island and New Hampshire. While some are more likely than others to pass such a law, the takeaway is more extensive, all-encompassing privacy and data security rights and requirements likely will soon be in place throughout much of the U.S.

While the VCDPA applies to Virginia residents, it reaches beyond Virginia's physical and cyber borders. That's because it applies not only to companies that own data regarding Virginia residents, it also covers companies that process data regarding Virginia residents. While there's a fairly broad Gramm-Leach-Bliley Act exemption, the VCDPA grants much more to consumers, including the right to correct and delete data, the right to opt out of targeted advertising, a new category of sensitive data, more requirements on processors (a.k.a. service providers), a requirement to minimize data collection, a requirement to perform data protection assessments, etc. There's a lot more there – but even so, many consumer advocates criticized the law because it didn't go far enough. The governor signed it on the premise it was best to get something on the books that could be amended or expanded from there. That sounds like California, so it would be no surprise if Virginia takes another bite at that apple next year, or if the Virginia attorney general tries to apply the GLBA exemption as narrowly as possible to cover only GLBA data.

Let's move on to data security. The FTC published a proposed rule updating the GLBA Safeguards Rule, which, of course, applies nationally to all dealers. The Safeguards Rule currently provides for

a principles-based approach to data security. A financial institution must maintain a written comprehensive information security program that provides for administrative, technical, and physical safeguards to ensure the privacy and security of customers' information, protect against anticipated threats or hazards to the security or integrity of customers' information and protect against unauthorized access to customers' information.

The rule the FTC is proposing is much more prescriptive. The proposed rule was first published in 2016, and I expect it to resurface as a final rule in some form during 2021. Here's a taste of what the proposed rule requires:

- Appointment of a "qualified" person with ultimate responsibility for data security (the current rule allows for more than one person).
- A formal risk assessment.
- Encryption of data, *at rest and in transit*.
- Multi-factor authentication for any individual accessing customer information.
- Audit trails to detect and respond to security events.
- Procedures to securely dispose of all forms of customer information no longer necessary for business operations or other legitimate business purposes.
- Change management procedures.
- Policies and procedures to monitor the activity of authorized users and detect unauthorized access or use of, or tampering with, customer information by such users.
- Regular testing and continuous monitoring of key controls, systems and procedures.
- Appropriate training, including verifying that key security personnel take steps to maintain current cybersecurity knowledge.
- Periodic assessments of service providers based on their information security risk.
- The establishment of an incident response plan.
- Annual reporting to the board of directors on issues related to the information security program.

Yes, there are a few exceptions – but not many. Overall, the proposed rule is a big lift. Re-examine your privacy and data security practices, policies and procedures, and keep your eyes wide open for what's coming down the pike. Privacy and data security will be developing and transforming over the next several years.