Automobile dealers and privacy law

John Yiokaris and Jason Brisebois

Like most other industries, the privacy policies and practices of automobile dealers are coming under increasing scrutiny in light of this increased focus on cyber security.

The Equifax and Starwood data breaches are only two of countless major news stories concerning data privacy to come to light over the course of the past year. Incidents like these have continued to put businesses of all sizes on alert to the dangers of failing to adequately protect customer data and follow Canadian privacy law. More than ever, privacy breaches raise major reputational and legal liabilities for companies of all sizes, with the actions of a few bad actors coupled with inadequate preparation by their targets leading to negative consequences that can reverberate through the target business for years to come.

Like most other industries, the privacy policies and practices of automobile dealers are coming under increasing scrutiny in light of this increased focus on cyber security. The consequences for a business failing to take preventative measures can be dire for auto dealers, and can lead to governmental investigations, fines, breaches of dealership agreements with their respective manufacturer, and even civil liability. The reputational fallout and bad press generated by data breaches and other violations of privacy law can create even larger issues than the immediate consequences, leaving a trail of reputational damage online and in the minds of consumers.

Even if a data breach has not yet occurred, dealers should not be lulled into a false sense of security or assume that such an incident couldn't happen to them. Data breaches can occur in all sizes and types of entities, ranging from the most sophisticated organizations (such as Marriot and Equifax) to local businesses, hospitals, and governmental departments. In this age of increasing connectivity, no parties are immune from the risks associated with collecting and storing highly-sensitive personal information of current and potential customers.

Data breaches can occur in many different ways: intentionally, unknowingly, carelessly, or through theft. Increasingly, companies should be turning their attention to not only planning for if a cyber attack or data breach occurs, but when one of these incidents occur. Attention must be given to how to manage such an incident as it is ongoing or has just transpired, but also how to manage this incident and its consequences long-term.

Auto dealers handle many different kinds of personal information that is subject to privacy protection laws: drivers' licences, social insurance numbers, bank account and credit card information, for example. Yet a crucial part of any automobile dealership also involves the responsible sharing of personal information with others. Although all entities are increasingly faced with a growing number of cyber risks, what risks should auto dealers be most concerned about? Auto dealers of all sizes should consider the following questions and their responses:

- How is customer information being used? What have they consented to? What have they not consented to?
- Are we running credit checks that comply with all applicable privacy laws? Detailed rules exist about credit checks, and unauthorized credit checks can lead to fines and liability under the Consumer Reporting Act and privacy legislation.
- Have you explained to customers and potential customers how their information will be used? Have you developed a privacy policy governing your use of their information that you can share with them?
- How long is personal information kept? Personal information may be retained only as long as necessary for the fulfillment of the purpose for which it was given. Does the dealership have in place guidelines for the destruction of personal information?
- What controls exist on employees accessing personal information of customers? Who is allowed to review the information? Do they need to have access? What do they need to access? Is their review authorized?
- Have you retained IT service providers that are well-versed in security matters and which can support all of your security and privacy needs?
- Have you reviewed which third-party vendors have been given access to your information technology systems? Have you vetted these vendors to ensure they understand the importance of maintaining data security and privacy at your dealership? Do they have their own checks and balances in place to ensure the same?
- How is personal information shared with the manufacturer and third party vendors?
- Does the dealership have policies or rules in place for downloading information to laptop computers, external hard drives or USB keys that could be easily lost or stolen? Stolen laptops with sensitive customer information may be a more significant concern than sophisticated online hackers.
- Has the dealership adequately ensured the physical security of the dealership premises and the electronic and hard-copy information and data contained onsite?
- Does your dealership have safeguards in place against external cybersecurity threats and the ability of third-parties to illicitly access customer information? Do you know what to do if a data breach occurs?
- Have you obtained adequate insurance coverage – both to cover your dealership from data breaches and other cybersecurity threats?

In addition to adequately protecting personal data stored at dealerships from theft or loss, dealers must also ensure that the solicitation and advertising they undertake also comply with Canada's applicable privacy and advertising legislation. Specifically, dealers should ensure they are in full compliance with Canada's anti-spam legislation ("CASL"). CASL prohibits businesses from sending via e-mail a business-related or commercial e-mail message unless the intended recipient of that message has explicitly or implicitly consented to receive it. Dealers should take special precautions to ensure that the intended recipient has either (a) expressly consented to receive the message, either verbally or in writing, or (b) implicitly consented to receive the message by carrying on an "existing business relationship" with the sender. The definition of an "existing business relationship" is highly technical, and is premised on whether particular activities between the sender and the recipient, such as previous commercial activity, contractual relationships, or inquiries have occurred between the parties before the communication in question. Automotive dealers should consult with legal counsel experienced in privacy and advertising law prior to soliciting customers and potential customers via e-mail to ensure they are not running afoul of CASL and other applicable Canadian privacy legislation. AW

John Yiokaris, Sotos LLP - John Yiokaris is a partner with Sotos LLP in Toronto, Canada's largest franchise law firm. He has been recognized by Chambers Canada, LEXPERT, Who's Who Legal, Lexology, and Best Lawyers Canada as a leading Canadian franchise law practitioner. John practices business law with a specific focus on the automotive industry, franchising, and disputes and he is trusted counsel to both automotive manufacturers and dealers. John can be reached directly at 416.977.3998 or jyiokaris@sotosllp.com.

Jason Brisebois, Sotos LLP - Jason Brisebois is an associate with Sotos LLP. He practices business law with a focus on franchising, distribution, and licensing. Jason can be reached directly at 416.572.7323 or jbrisebois@sotosllp.com