209 Battery Street | PO Box 988 | Burlington, VT | 05402 | 802.864.5751

MEMORANDUM

To: Vermont Vehicle & Automotive Distributors Association

From: Joshua R. Diamond, Esq.

Date: July 23, 2024

Re: Security Breach Obligations

CDK, which provides dealer management services, was subject to a ransomware attack on or about June 19, 2024. The security incident resulted in the inoperability of CDK's services to Vermont automobile dealerships. CDK's systems maintained customer information on behalf of Vermont automobile dealers that may be considered personal identifiable information. Under Vermont law there are notice obligations in the event of a security breach. Currently, it is unknown whether the ransomware attack resulted in the acquisition of personal identifiable information that would constitute a security breach.

The Vermont Vehicle & Automotive Distributors Association has requested that Dinse, P.C., provide an overview of the Vermont Security Breach Notice Act, 9 V.S.A. §§ 2430, 2435, that may be implicated by this ransomware attack.

Overview of Vermont's Security Breach Notice Act

Businesses that possess personal identifiable information or login credentials of Vermont consumers have notice obligations in the event of a security breach. Here are the key definitions and obligations under the Vermont Security Breach Notice Act.

1. **Personal identifiable information** includes a person's name (first name or initial and last name) and one of the following: social security number; driver's license number, passport number, or other government identification number; financial account number (if account could be accessed without a passcode); passcode for a financial account; biometric data; genetic information; and health care information. 9 V.S.A. § 2430(10)(A).

2. **Security Breach** occurs when there is an unauthorized acquisition of electronic data or a **reasonable belief** that there has been an unauthorized acquisition that compromises the security, confidentiality, or integrity of a **consumer's personal identifiable information** or login credentials. 9 V.S.A. § 2430(13)(A). Factors to consider whether there is a reasonable belief that an unauthorized acquisition has occurred include, but are not limited to:

> a. indications that information is in the physical possession and control of a person without valid authorization, such as a lost or stolen computer or other device containing information;
>
> b. indications that the information has been downloaded or copied;
>
> c. indications that the information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported.

9 V.S.A. § 2430(13)(C). These factors are not exhaustive. The Vermont Attorney General's Office, *Vermont Security Breach Notice Act Guidance* (2020), offers other examples of a reasonable belief that a security breach occurred. This includes the existence of ransomware that is known to exfiltrate data. *Id.*, at § 7.

Not all ransomware incidents are security breaches. If the ransomware attack merely encrypts a hard drive that effectively locks an owner/user out of the system, then it may not be a security breach. The question is whether there is information that indicates that the ransomware attack has the ability to exfiltrate or otherwise access PII. Vermont Attorney General's Office, *Vermont Security Breach Notice Act Guidance,* at § 47 (2002).

It is noted that the reasonable discovery of a security breach is not the date that an investigation is completed, it is the earliest date that an entity became aware of, or had a reasonable belief of, unauthorized activity. Vermont Attorney General's Office, *Vermont Security Breach Notice Act Guidance,* at § 47 (2002).

3. General notice requirements.

Notice of the date of the security breach, the date of discovery of the data breach, and a description of the data breach shall be provided to the Attorney General's Office within 14 days of the discovery or its reasonable belief. 9 V.S.A. § 2435(b)(3). Notice to the Vermont consumer shall occur within 45 days of the discovery or notice of the security breach. 9 V.S.A. § 2435(b)(1).

Notice to the three major credit bureaus shall occur if the security breach involves a more than a 1000 Vermont consumers. 9 V.S.A. § 2435(c).

4. Notice requirements involving a breach by the licensee of data.

This security incident involves a third party, CDK, who presumably has a license to utilize the VADA members' data. Regardless, Vermont automobile dealers will have a responsibility to provide notice if it involves data involving the dealers' customers. The Vermont Attorney General's Office has opined that when there is a breach, and multiple parties have owned, controlled or possessed PPI subject to the breach, all parties have an obligation to provide notice. Vermont Attorney General's Office, *Vermont Security Breach Notice Act Guidance,* at § 47 (2002).

This memo provides a general overview of the obligations under the Vermont Security Breach Notice Act. Individual automobile dealers are encouraged to contact their attorneys for further information and details such as the scope of information contained in the notice, the method of delivery for the respective notice to consumers, and obligations to remedy a security breach.