Akin®

Vermont Attorney General Provides Guidance on Security Breach Notice Act

Jul 27, 2020

Reading Time : **2 min**

By: Natasha G. Kohne, Rebecca Kocsis (Legal Project Analyst)

The AG's guidance notes that it is not directed to entities regulated by the Vermont Department of Financial Regulation (DFR) (the Act mandates that data collectors report security breaches not only to affected consumers, but also to the AG or DFR, depending on whether they are regulated by the DFR or not). However, the guidance still provides helpful interpretations and applications of the Act that, while not legal advice, may shed light into how data collectors may best comply with the Act to avoid enforcement actions.

The guidance is organized as a set of helpful FAQ questions to assist data collectors determine if they are subject to the Act and provides a quick-reference guide for what to do if you are a business or state agency that has suffered (or suspects to have suffered) a data security breach. However, these steps should be viewed with caution, as they are written from the perspective of complying with the Act to avoid an AG enforcement action, and not necessarily to avoid civil litigation from consumers, vendors or even employees. Thus, data controllers should consult with outside counsel in the early stages of investigating a breach to ensure that proper protections are in place to minimize the risk of litigation and protect attorney-client communications.

Some of the most important takeaways from the guidance include real-world examples for determining what constitutes "personally identifiable information" (PII) under the recently amended Act, which included a substantive expansion to the definition of PII, whether a security breach has occurred and other key considerations. For example, in explaining the 45-day time limit to notify consumers of a breach, which starts when the data controller "discovers or is notified" of a breach, the AG provides numerous examples of scenarios that could start the notification clock. **Importantly, the guidance explicitly provides that the**

"discovery date 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."[1] Data controllers should thus have adequate policies and procedures in place to swiftly detect and report indicators of compromise or respond to external notifications of a potential breach.

We recommend that data collectors review the guidance in detail—whether or not they are located in Vermont—to become familiar with the Act's strict requirements and the most common violations as noted by the AG. If you have any questions about your company's obligations and compliance efforts, please contact a member of the Akin Gump Cybersecurity, Privacy and Data Protection team.

---

[1] This point is reemphasized in another discussion of the deadlines, in which the AG notes "The 45-day outer limit incorporates the time it will take to conduct an investigation – it does not begin after the investigation is completed."

Categories

State Privacy Policy | Data Breach