Consumer Data Industry Association
1090 Vermont Ave., NW, Suite 200
Washington, D.C. 20005-4905

Writer's email: mcarone@cdiaonline.org
Writer's direct dial: +1 (860) 836-2623

CDIAONLINE.ORG

March 23, 2023

House Bill 2077 – "An Act Concerning information technology" – Opposed Unless Amended

Dear Chair Billinger, Vice-Chair Claeys and members of the Senate Committee on Ways and Means,

On behalf of the Consumer Data Industry Association ("CDIA"), I want to offer comments regarding House Bill 2077 – "An Act Concerning information technology".

The Consumer Data Industry Association is the voice of the consumer reporting industry, representing consumer reporting agencies including the nationwide credit bureaus, regional and specialized credit bureaus, background check and residential screening companies, and others.

House Bill 2077 as amended in the House of Representatives would require that any entity that transmits, receives, processes or stores personal information that is provided by the state of Kansas or supports information systems operated by the state of Kansas or any governmental entity that accesses information systems operated by the state of Kansas that has a significant cybersecurity incident shall, not later than 12 hours after the discovery of the significant cybersecurity incident, notify the Kansas information security office and, if the significant cybersecurity incident involves election data, the secretary of state.

The bill's definition of a "significant security incident" is very broad and even includes instances where no incident actually occurred, such as a "suspected breach". The definition essentially covers anything a company would investigate and must respond to. It goes far beyond if an actual incident occurred or not.

The 12 hour reporting time frame of a significant security incident will be an impossible standard to meet. We have seen some states with a 2 day notice for companies that are operating under a contract for certain data. However, that only applies when an actual breach has occurred and it does not pertain to an incident, attempt or suspected breach.

The reporting requirement in this bill coupled with the broad definition of a "significant security incident" would also create a very significant number of reports to the Kansas Information Security Office (KISO). A study from the University of Maryland found there was an average of 2,244 attacks each day, which breaks down to nearly 1 cyberattack every 39 seconds.[1]

It would be extremely difficult, if not impossible, for both companies and a state agency to report every attempt and process the volume of such reports that would ensue from this broad definition and extremely short reporting requirement.

For these reasons above, CDIA opposes the bill as currently drafted and respectfully requests the bill to be amended. Thank you for the consideration of our comments and I would be happy to answer any questions you may have.

Sincerely,

Mike Carone

Mike Carone,

Manager of Government Relations

Consumer Data Industry Association (CDIA)

1 Cukier, Michel. Study: Hackers Attack Every 39 Seconds, University of Maryland, https://eng.umd.edu/news/story/study-hackers-attack-every-39-seconds.