ASSEMBLY THIRD READING
AB 1035 (Mayes)
As Amended April 22, 2019
Majority vote

SUMMARY:

This bill requires a person, business, or agency that owns or licenses computerized data that includes personal information (PI) to disclose a breach of the system within 45 days, as specified.

Major Provisions

COMMENTS:

Existing law requires that individuals are notified of a breach "in the most expedient time possible and without unreasonable delay" (*See* Civil Code Sections 1798.29(a) and 1798.82(a)). This bill would instead require the disclosure be provided to affected persons in the most expedient time possible and without unreasonable delay, but in no case more than 45 days following a data breach. According to the Attorney General's (AG) most recent data breach report, the average time from discovery of a breach to notification of those affected was 40 days, and the median was 30 days. In 25% of the breaches consumers were notified in 16 days or less, and in 75% of them notification was made in 50 days or less (California Department of Justice, *California Data Breach Report,* (Feb. 2016) https://oag.ca.gov/sites/all/files/agweb /pdfs/dbr/2016-data-breach-report.pdf >[as of Apr. 21, 2019]).

Despite the average times reported by the AG above, many companies take much longer to notify individuals that their information may have been stolen, thus denying those affected the opportunity to proactively begin mitigating the risks of identity theft and fraud. For example, when the PI of at least 30,000 Kaiser employees was negligently released in 2011, Kaiser waited nearly six months before notifying affected individuals. According to the AG, this constituted unreasonable delay (*See* Breaux et al, *California AG Cracks Down on Timing of Data Breach Disclosures*, Haynesboone, (Feb. 5, 2014)). To ensure that affected persons learn that their PI has been compromised in a timely manner, this bill would require that data breach disclosures are made in the most expedient time possible and without unreasonable delay, but in no case more than 45 days from the discovery of the breach. This language will also ensure that if disclosure can be made earlier, the business or agency would be required to make the disclosure "in the most expedient time possible." Taking note of the average timeframes referenced by the AG above, the vast majority of breach notifications are already happening within this timeframe. Accordingly, this requirement should not be overly burdensome on business, but would ensure that disclosures are made in a reasonable amount of time so that individuals whose PI has been compromised can take appropriate steps to protect themselves from identity theft and fraud.

According to the Author:
In the absence of a uniform federal law, current California law since 2003 has required data breach disclosures to be "made in the most expedient time possible and without unreasonable delay," while also working with law enforcement needs. Companies have taken this statute to mean a variety of things. For example, in late September of 2018, Facebook reported within 72 hours that hackers could have accessed the data from tens of millions of accounts, despite the

company not yet knowing the full extent of the breach. They immediately logged out up to 90 million users from their accounts and required them to reenter their information. Conversely, Google learned of a data breach that affected half a million accounts in March of 2018, but did not disclose the breach until October of 2018.

Arguments in Support:
None on file.

Arguments in Opposition:
The Consumer Attorneys of California (CAOC) write in opposition unless amended, "[e]xisting law requires businesses to notify affected individuals "in the most expedient time possible and without unreasonable delay." Most state breach laws (85%) have essentially the same notification timing provision as California. However, we know most companies do not notify in the most expedient time possible and many fail to notify at all. It is essential that consumers receive notice of a data breach as soon as possible so that they can take steps to protect themselves from identity theft, see attached risks of identity theft. […] If California is to enact an outer limit, CAOC urges that limit be the most protective possible. Current California law requires hospitals and medical entities to notify patients of a data breach within 15 business days. If hospitals can notify of medical data breaches within 15 business days, companies that maintain and sell our data should be held to the same standard."

FISCAL COMMENTS:

None

VOTES:

ASM PRIVACY AND CONSUMER PROTECTION: 10-0-1
YES: Chau, Bauer-Kahan, Berman, Calderon, Gabriel, Gallagher, Irwin, Obernolte, Smith, Wicks
ABS, ABST OR NV: Kiley

UPDATED:

VERSION: April 22, 2019

CONSULTANT: Nichole Rapier / P. & C.P. / (916) 319-2200 FN: 0000380