

New Jersey revises data breach law, expands definition of personal information to include online account information



James J. Giszczak, Dominic A. Paluzzi | Monday, June 3, 2019

On May 10, 2019, New Jersey Gov. Phil Murphy signed Assembly Bill 3245 into law. AB 3245 expands the definition of “personal information” under the state data breach statute and addresses electronic notification in the event that a data breach involves a username or password.

New Jersey requires individuals to be notified in the event of a breach of security involving personal information that compromises the security, confidentiality, or integrity of personal information. Previously, New Jersey had defined personal information to include an individual’s first and last name, along with any of the following data elements: Social Security number; driver’s license number or state identification number; or account number or credit card number in combination with any required security code, access code, or password that would permit access to an individual’s financial account.

AB 3245 amends the definition of personal information to include “an individual’s user name, email address, or any other account holder identifying information, in combination with any password or security question and answer that would permit access to an online account.”

Accordingly, in the event that a breach of security includes a New Jersey resident’s name and online account information, the individual must be notified under New Jersey law.

AB 3245 also addresses the delivery of notification in the event of a breach including such personal information. In the event of a breach of security that includes a New Jersey resident’s name and online

New Jersey revises data breach law, expands definition of personal information to include online account information

account information, the business that experienced the breach may provide notification electronically or other form that directs the resident to change any impacted credentials, or to take other steps in order to protect the account and any other account that may use the same credentials. However, AB 3245 prohibits a business from sending an electronic notification to an email account which had credentials impacted by the breach.

Businesses that collect and store usernames, email addresses or other online credentials in an unencrypted or unredacted format should be aware of these recent changes and should update their incident response plans and procedures accordingly. AB 3245 becomes effective September 1, 2019.



James J. Giszczak



Dominic A. Paluzzi