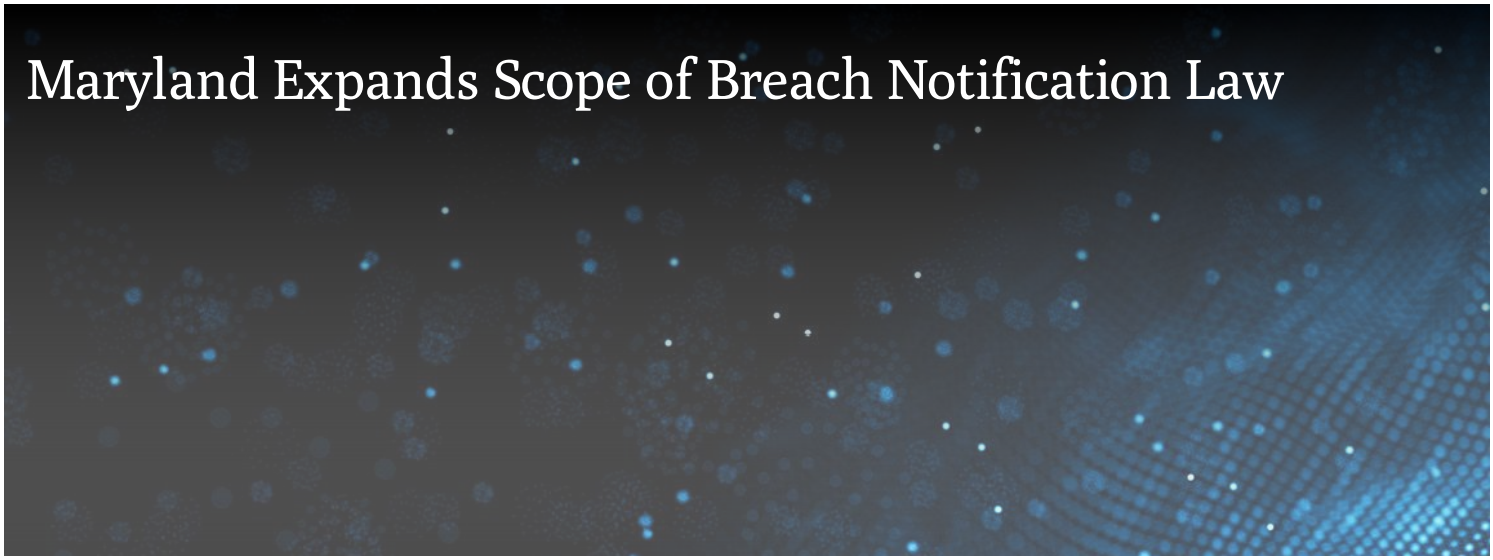
WINSTON & STRAWN LLP

BLOG

Maryland Expands Scope of Breach Notification Law



OCTOBER 11, 2017

Maryland amended its data breach notification law to, among other things, expand on its definition of "personal information" covered under the law. Under the law's new definition, a full list of personal information that—in combination with a person's first name, or initial and last name—would trigger notification obligations includes:

1. A social security number, an individual taxpayer identification number, a passport number, or other identification number issued by the federal government;
2. A driver's license number or state identification card number;
3. An account number, a credit card number, or a debit card number, in combination with any required security code, access code, or password, that permits access to an individual's financial account;
4. Health information, including information about an individual's mental health;
5. A health insurance policy or certificate number or health insurance subscriber identification number, in combination with a unique identifier used by an insurer or an employer that is self-insured, that permits access to an individual's health information; or
6. Biometric data of an individual generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, voice print, genetic print, retina or iris image, or other unique biological characteristic, that can be used to uniquely authenticate the individual's identity when the individual accesses a system or account.

The amendments, which go into effect January 1, 2018, also include Maryland in a growing number of jurisdictions (California, Florida, Illinois, Maine, Nebraska, Nevada, Rhode Island, Puerto Rico, and Wyoming) that define personal information to include an individual's user name or email address when in combination with a password or security answer that permits access to the individual's email account. When a breach involves only an individual's email account information and no other personal information, the amendments allow for notification to affected individuals that instructs them to change their password and security question settings or other take steps appropriate to protect their email account and other online accounts that share a password. However, organizations may not provide notification to individuals via an email account whose credentials were involved in a breach unless the organization is able to verify that the individual has logged onto the account through an IP address or online location from which the organization knows the individual customarily accesses the account.

Finally, while Maryland previously required notification of a breach "as soon as reasonably practicable," under the amendments, notification is now required no later than 45 days after learning of a breach. If notification is delayed due to an investigation by law enforcement, notification is now required within 30 days after law enforcement determines that notification will not impede the investigation.

TIP: Companies should keep in mind that state legislatures continue to tweak and modify their breach notification laws. As demonstrated by Maryland's amendments, these tweaks often serve to expand the scope of the state's breach notification requirements and impose more stringent notification obligations.

2 Min Read

Author

Eric Shinabarger

Related Locations

Chicago

Related Topics

Online Privacy | Data Breach | Consumer Privacy | Financial Privacy | Biometrics

Related Capabilities

Privacy & Data Security | Advertising Litigation

Related Professionals

Eric Shinabarger

This entry has been created for information and planning purposes. It is not intended to be, nor should it be substituted for, legal advice, which turns on specific facts.