Alert

October 9, 2024

COZEN O'CONNOR

Amendments Expand Pennsylvania's Data Breach Notification Law

Businesses suffering a data breach affecting Pennsylvania residents may have new compliance obligations pursuant to a recent amendment to the Commonwealth's data breach notification law. Earlier this year, Pennsylvania lawmakers enacted a bill amending the state's Breach of Personal Information Notification Act (BPINA). Those changes came into effect on September 26 (the September Amendments) and represent the second update to BPINA in two years. The September Amendments contain several significant changes to the law, including imposing new obligations and reporting requirements on companies that have experienced a breach.

Required Notice to the Attorney General

Unlike the data breach reporting laws of many other states, BPINA had previously not imposed any requirement that the state Attorney General be notified in the event of a breach. That changed when the September Amendments came into effect—the AG must now be notified of any breach affecting more than 500 Pennsylvania residents. The notification must include certain information, including a summary of the breach incident and an estimate of the total number of impacted individuals.

The September Amendments do not specify how a breached entity must notify the AG. However, in response to the changes and in preparation for the new notice requirement, the AG's office announced the release of an online portal via which companies could report breaches.

The September Amendments also updated the threshold for providing notification to consumer reporting agencies—entities like Equifax, Experian, and Transunion—from 1,000 to 500 people.

Credit Monitoring

The September Amendments also impose a new requirement that, under certain circumstances, breached entities provide one year of credit monitoring services to impacted individuals. Companies must offer credit monitoring to individuals whose first and last names were exposed in combination with either:

1. their social security number,
2. their bank account number and/or
3. their driver's license or state ID number.

While every state has a data breach notification law, Pennsylvania is only the sixth jurisdiction to require credit monitoring, joining California, Connecticut, Delaware, Massachusetts, and DC. These other laws only require credit monitoring in circumstances where social security numbers or, in California, Connecticut, and DC, certain other government-issued ID numbers are included in the breach. Pennsylvania is the first to require credit monitoring based on the exposure of bank account numbers.

Overall, the September Amendments represent a set of significant updates to BPINA. While state AG notification is a fairly common requirement among data breach notification laws, an obligation to offer credit monitoring is not. Companies handling Pennsylvanians' personal Information, particularly those handling information covered by the credit monitoring requirement, should carefully evaluate how these changes may impact their obligations in the event of a data breach.

Benjamin Mishkin

Member

bmishkin@cozen.com
Phone: (215) 665-2171
Fax: (215) 372-2407

Daniel Kilburn

Associate

DKilburn@cozen.com
Phone: (215) 665-4726
Fax: (215) 665-2013

Related Practice Areas

- Business
- Technology, Privacy & Data Security