Knox McLaughlin Gornall & Sennett, P.C.
Erie • Pittsburgh • Jamestown, NY
814-459-2800 • www.kmgslaw.com

Pennsylvania Breach of Personal Information Notification Obligations

Posted on March 08, 2018

In addition to various Federal requirements such as the Health Insurance Portability and Accountability Act (HIPAA) that impose obligations on entities to disclose the occurrence of data breaches involving personal information, **Pennsylvania law imposes breach notification requirements.**

73 P.S. Chapter 43 sets forth the Breach of Personal Information Notification Act (73 P.S. Section 2301 et. seq.). This Act identifies the entities subject to the notification law, the protected data, the persons to whom notice must be given, when the notice must be given and the authority of the Pennsylvania Attorney General to enforce a violation as an unfair trade practice.

Following is a summary of the Act.

Covered Entities and Personal Information

The Act extends to any *entity* that maintains, stores or manages computerized data that includes *personal information*. “Entity” is broadly defined to include a Pennsylvania state agency or political subdivision, an individual or business doing business in Pennsylvania.

“Personal Information” is an individual’s first name or initial and last name in combination with and linked to any one or more of the following data elements when the data elements are not encrypted or redacted:

- Social Security number
- Driver’s license number or a State identification card number issued in lieu of a driver’s license
- Financial account number, credit or debit card number, in combination with any required security code, access code or password that would permit access to an individual’s financial account

Breach of Data Security and Persons to Whom Notice Must Be Given

A covered entity must give notice of a *breach of the security of the system* which is defined as the unauthorized access and acquisition of computerized data that materially compromises the security or confidentiality of personal information maintained by the entity as part of a database of personal information regarding multiple individuals and that causes, or the entity reasonably believes has caused or will cause, loss or injury to any Pennsylvania resident. Access to and use of the data by entity employees in the scope of employment and for the proper business purposes of the covered entity are not breaches of the security system. Each Pennsylvania resident whose unencrypted or un-redacted personal information was, or was reasonably believed to have been, accessed by an unauthorized person should be given notice of the breach.

Notice

Except for delays requested to meet the needs of law enforcement or in order to take necessary measures to determine the scope of the breach and to restore the reasonable integrity of the data system, the notice shall be made without unreasonable delay to Pennsylvania residents.

Residency may be determined by the individual's principal mailing address, as reflected in the entity's computerized data. Notice may be provided by any of the following methods:

- Written notice to the last known home address for the individual
- Telephonic notice, if the customer can be reasonably expected to receive it and the notice is given in a clear and conspicuous manner, describes the incident in general terms and verifies personal information but does not require the customer to provide personal information and the customer is provided with a telephone number to call or Internet website to visit for further information or assistance
- Email notice, if a prior business relationship exists and the person or entity has a valid e-mail address for the individual

A substitute form of notice is permissible if the entity demonstrates one of the following:

- The cost of providing notice would exceed $100,000;
- The affected class of subject persons to be notified exceeds 175,000; or
- The entity does not have sufficient contact information.

The form of substitute notice shall consist of all of the following:

- Email notice when the entity has an email address for the subject persons;
- Conspicuous posting of the notice on the entity's Internet website if the entity maintains one; and
- Notification to major statewide media.

Enforcement

A violation of the Act is deemed to be an unfair or deceptive practice in violation of the Pennsylvania Unfair Trade Practices and Consumer Protection Law, which is enforced by the Pennsylvania Attorney General. Although there is no private right of action under the Pennsylvania Breach of Personal Information Notification Act, compliance will go a long way toward mitigating individual damages and the private claims under other causes of action that will surely follow. In addition to the Pennsylvania requirements, most other states have similar breach notification laws protecting the residents of those jurisdictions.

Conclusion

Any entity storing personal information must, at a minimum: have, maintain and monitor its data security systems; regularly conduct security assessments; develop and constantly improve its data privacy policies and practices; and be prepared with incident response plans.

Compliance with applicable federal and state law disclosure requirements must be part of the planning.
