Babst | Calland
Attorneys at Law

ALERT
PUBLIC SECTOR

Governor Wolf Signs Act 151 Addressing Data Breaches Within Local Entities

On Thursday, November 3, 2022, Governor Tom Wolf signed PA Senate Bill 696, also known as Act 151 of 2022 or the Breach of Personal Information Notification Act. Act 151 amends Pennsylvania's existing Breach of Personal Information Notification Act, strengthening protections for consumers, and imposing stricter requirements for state agencies, state agency contractors, political subdivisions, and certain individuals or businesses doing business in the Commonwealth. Act 151 expands the definition of "personal information," and requires Commonwealth entities to implement specific notification procedures in the event that a Commonwealth resident's unencrypted and unredacted personal information has been, or is reasonably believed to have been, accessed and acquired by an unauthorized person. The requirements for state-level and local entities differ slightly; this *Alert* will address the impact of Act 151 on local entities. While this law does not take effect until May 22, 2023, it is critical that all entities impacted by this law be aware of these changes.

For the purposes of Act 151, the term "local entities" includes municipalities, counties, and public schools. The term "public school" encompasses all school districts, charter schools, intermediate units, cyber charter schools, and area career and technical schools. Act 151 requires that, in the event of a security breach of the system used by a local entity to maintain, store, or manage computerized data that includes personal information, the local entity must notify affected individuals within seven business days of the determination of the breach. In addition, local entities must notify the local district attorney of the breach within three business days.

The definition of "personal information" has been updated, and includes a combination of (1) an individual's first name or first initial and last name, and (2) one or more of the following items, if unencrypted and unredacted:

- Social Security number;
- Driver's license number;
- Financial account numbers or credit or debit card numbers, combined with any required security code or password;
- Medical information;
- Health insurance information; or
- A username or password in combination with a password or security question and answer.

The last three items were added by this amendment. Additionally, the new language provides that "personal information" does not include information that is made publicly available from government records or widely distributed media.

NOVEMBER 29, 2022

CONTACT

MICHAEL T. KORNS
MKorns@babstcalland.com
412.394.6440

EMBER K. HOLMES
EHolmes@babstcalland.com
412.394.5492

Pittsburgh, PA
Two Gateway Center
603 Stanwix Street
Sixth Floor
Pittsburgh, PA 15222
412.394.5400

BABSTCALLAND.COM

Act 151 defines previously undefined terms, drawing a distinction between "determination" and "discovery" of a breach, and setting forth different obligations relating to each. "Determination," under the act, is defined as, "a verification or reasonable certainty that a breach of the security of the system has occurred." "Discovery" is defined as, "the knowledge of or reasonable suspicion that a breach of the security of the system has occurred." This distinction affords entities the ability to investigate a potential breach before the more onerous notification requirements are triggered. A local entity's obligation to notify Commonwealth residents is triggered when the entity has reached a determination that a breach has occurred. Further, any vendor that maintains, stores, or manages computerized data on behalf of a local entity is responsible for notifying the local entity upon discovery of a breach, but the local entity is ultimately responsible for making the determinations and discharging any remaining duties under Act 151.

Another significant update afforded by Act 151 is the addition of an electronic notification procedure. Previously, notice could be given: (1) by written letter mailed to the last known home address of the individual; (2) telephonically, if certain requirements are met; (3) by email if a prior business relationship exists and the entity has a valid email address; or (4) by substitute notice if the cost of providing notice would exceed $100,000, the affected class of individuals to be notified exceeds 175,000, or the entity does not have sufficient contact information. Now, in addition to the email option, entities can provide an electronic notice that directs the individual whose personal information may have been materially compromised to promptly change their password and security question or answer, or to take any other appropriate steps to protect their information.

Act 151 also provides that all entities that maintain, store, or manage computerized personal information on behalf of the Commonwealth must utilize encryption – this provision originally applied only to employees and contractors of Commonwealth agencies, but was broadened in Act 151. Further, the act provides that all entities that maintain, store, or manage computerized personal information on behalf of the Commonwealth must maintain policies relating to the transmission and storage of personal information – such policies were previously developed by the Governor's Office of Administration.

Finally, under Act 151, any entity that is subject to and in compliance with certain healthcare and federal privacy laws is deemed to be in compliance with Act 151. For example, an entity that is subject to and in compliance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) is deemed compliant with Act 151.

Although Act 151 is an amendment to prior legislation, the updates create potential exposure for local entities and the vendors that serve them. For local municipalities, schools, and counties, compliance will require a proactive approach – local entities will have to familiarize themselves with the new requirements, be mindful of the personal information they hold, and ensure that their vendors are aware of their obligations. Further, local entities will be required to implement encryption protocols, and prepare and maintain storage and transmission policies. If you have questions about how Act 151 will impact your organization, please contact Michael Korns at 412-394-6440 or mkorns@babstcalland.com or Ember Holmes at 412-394-5492 or eholmes@babstcalland.com.