# PA Changed Its Data Breach Law. Municipalities Are In The Crosshairs. Are You Ready?

**PA State Association of Boroughs**
Fall Conference
October 14, 2023

Presented by:

**Sandy Garfinkel**
*Co-Chair, Privacy & Data Security Group*
***McNees Wallace & Nurick LLC***

© McNees Wallace & Nurick LLC

# Key Impacts of PA Breach Notification Law Amendments

- Expands types of information that trigger notification duties
- Clarifies when the notification clock begins ticking
- Compresses timing for breach reporting/notification for municipalities, counties, public schools, state agencies and state agency contractors
- Creates new data security requirements for those with access to Commonwealth information


© McNees Wallace & Nurick LLC

# The Patchwork of Notification Requirements

1. 50 U.S. state data breach notification laws
2. Federal laws (industry specific)
    a. HIPAA/HITECH Act (health care providers/insurers)
    b. Privacy Act and Federal Information Security Management Act (public sector)
    c. Gramm-Leach-Bliley Act (financial institutions)
3. Approximately 109 foreign data privacy laws and regulations
    a. GDPR and Privacy Shield (EU)
    b. PIPEDA (Canada)
4. Contractual requirements


© McNees Wallace & Nurick LLC

# PA Breach of Personal Information Notification Act (BOPINA)

An entity that maintains, stores or manages computerized data that includes personal information shall provide notice of any breach of the security of the system following discovery of the breach of the security of the system to any resident of this Commonwealth whose unencrypted and unredacted personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person.

- 50 states (plus PR, VI) have similar breach notification laws


© McNees Wallace & Nurick LLC

# Pennsylvania Breach Of Personal Information Notification Act – The “Old” Version

- "Entity" means a state agency, a political subdivision of the Commonwealth of PA, or an individual or business doing business in PA
- Duty of notification rests with the entity even if information is stored or otherwise entrusted to a third-party vendor (contractors or "on the cloud")
- No private cause of action under act
  - ✓ Violations deemed to be an unfair trade practices; A.G. has exclusive authority to bring action under UTPCPL for violation
  - ✓ Civil penalties of up to $1,000 per violation, plus costs and restitution in court's discretion


© McNees Wallace & Nurick LLC

# Pennsylvania Breach Of Personal Information Notification Act - The “Old” Version

Definition of PII:

- An individual's first name or first 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:
  - (i) Social Security number.
  - (ii) Driver's license number or a State identification card number.
  - (iii) 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.


© McNees Wallace & Nurick LLC

# Pennsylvania Breach Of Personal Information Notification Act - NEW

## Expanded Definition of PII

Effective May 2, 2023

- An individual's first name or first 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:
  - (iv) “Medical information,” which is defined as “Any individually identifiable information contained in the individual’s current or historical record of medical history or medical treatment or diagnosis created by a healthcare professional.”
  - (v) “Health insurance information,” which is defined as “An individual’s health insurance policy number or subscriber number in combination with access code or other medical information that permits misuse of an individual’s health insurance benefits.”
  - (vi)“Username or e-mail address, in combination with a password or security question that would permit access to an online account”


© McNees Wallace & Nurick LLC

# Pennsylvania Breach Of Personal Information Notification Act

- Trigger: "Breach of the security of the system" means:
  - 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 PA resident.


© McNees Wallace & Nurick LLC

# Compare and Contrast: Breach Notification Triggers

- Notification triggered by any “unauthorized access” (CT, FL, NJ, PR)
- Notification only if determined that incident “reasonably likely to cause substantial harm to consumers” (43 states, including PA)
  - Or, “material compromise” (AZ)
  - Or, notification unless determined that misuse of personal information has not occurred and is not likely to occur (CO)
  - Or, notification required if misuse of personal information for identity theft or fraud purposes has occurred, or is reasonably likely to occur (UT)



© McNees Wallace & Nurick LLC

# Compare and Contrast: Breach Notification Triggers

- HIPAA Breach Notification Rule: Impermissible use or disclosure of PHI is presumed to be a breach unless the covered entity or business associate demonstrates that there is a low probability that PHI has been compromised based on a risk assessment of at least the following factors:
  - The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;
  - The unauthorized person who used the protected health information or to whom the disclosure was made;
  - Whether the protected health information was actually acquired or viewed; and
  - The extent to which the risk to the protected health information has been mitigated.


© McNees Wallace & Nurick LLC

# Pennsylvania Breach Of Personal Information Notification Act

- Time for notice:
  - Except as provided in section 4 or in order to take any measures necessary 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.
    - Section 4.  Exceptions. The notification required by this act may be delayed if a law enforcement agency determines and advises the entity in writing specifically referencing this section that the notification will impede a criminal or civil investigation. The notification required by this act shall be made after the law enforcement agency determines that it will not compromise the investigation or national or homeland security.


© McNees Wallace & Nurick LLC

# Pennsylvania Breach Of Personal Information Notification Act

- Time for notice:
  - A county, public school, or municipality must provide notice to individuals within seven business days following the determination of a breach and must provide notice to the District Attorney in the county where the breach occurred within three business days following the determination of a breach.
    - "Public school" means any school district, intermediate unit, charter school, cyber charter school, or area career and technical school.


© McNees Wallace & Nurick LLC

# Pennsylvania Breach Of Personal Information Notification Act

## Amendments Effective May 2023

- Time for notice:
  - “Determination” 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 a reasonable suspicion that a breach of the system has occurred.”
  - Notification may be delayed “in order to take any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the data system.”


© McNees Wallace & Nurick LLC

# Pennsylvania Breach Of Personal Information Notification Act

## Amendments Effective May 2023

- Time for notice:
  - If a state agency determines that it is the subject of a breach of the security of the system affecting personal information maintained by the state agency or state agency contractor, the state agency shall provide notice of the breach of the security of the system within 7 business days following determination of the breach. Notification shall be provided concurrently to the Office of Attorney General.
  - A state agency contractor, defined as "A person, business, subcontractor, or third-party subcontractor that has a contract with a state agency for goods or services that requires access to personal information for the fulfillment of the contract" must now provide notice to the Chief Information Security Officer, or a designee of the State Agency, as soon as reasonably practicable after the discovery of a breach.


© McNees Wallace & Nurick LLC

# Compare and Contrast: Time for Notifications

| Timing to Notify Residents | States |
|---|---|
| Within 30 days of breach | CO<br>FL (plus additional 15 days for good cause shown) |
| No later than 45 days after discovery of breach | AL, MD, NM, OH, RI, TN, WA, WI, VT |
| No later than 60 days after discovery of breach | DE, SD, LA |
| Within 90 days after discovery of breach (unless delayed for a law enforcement investigation) | CT |
| Most expedient time possible and without unreasonable delay | AK, AZ, AR, CA, CO, DE, D.C., GA, HI, ID, IL, IN, IA, KS, KY, LA, ME, MA, MI, MN, MS, MO, MT, NE, NM, NV, NH, NJ, NY, NC, ND, OR, PA, RI, SC, TX, UT, VA, WA, WY<br><br>NOTE: CA guidance document recommends notifying within 10 business days. |
| As soon as reasonably practicable after discovery of breach | MD, OK, WV |



© McNees Wallace & Nurick LLC

# Pennsylvania Breach Of Personal Information Notification Act

- Who receives notice?
  - Each affected individual, plus:
  - When an entity provides notification under this act to more than 1,000 persons at one time, the entity shall also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis of the timing, distribution and number of notices.


© McNees Wallace & Nurick LLC

# Compare and Contrast: Who receives notice?

- Most states require notice to credit reporting agencies
- Most states require that notice be provided to the state's Attorney General or another state regulator if notice is given to more than 500 or 1,000 residents of the state



© McNees Wallace & Nurick LLC

# Form of Notice

- Notice may be provided by any of the following methods of notification:
  1. Written notice to the last known home address for the individual.
  2. 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.
  3. E-mail notice, if a prior business relationship exists and the person or entity has a valid e-mail address for the individual.


© McNees Wallace & Nurick LLC

# Form of Notice

- Notice may be provided by any of the following methods of notification:
  4. Substitute notice, 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.
     - The entity does not have sufficient contact information.

     Substitute notice shall consist of all of the following:

     a) E-mail notice when the entity has an e-mail address for the subject persons.

     b) Conspicuous posting of the notice on the entity's Internet website if the entity maintains one.

     c) Notification to major Statewide media.



© McNees Wallace & Nurick LLC

# Content of Notice

- Pennsylvania: unspecified
- Most states:
    1. The name and contact information of the business.
    2. A list of the types of PII believed to be breached.
    3. The date or estimated date of the breach, if known.
    4. Whether notification was delayed as a result of a law enforcement investigation.
    5. A general description of the incident.
    6. The toll-free telephone numbers and addresses of the major credit reporting agencies

Notification may include the following:

1. Information about what the business has done to protect individuals whose information has been breached.
2. Advice on steps that the person may take to protect themselves from the breach.


© McNees Wallace & Nurick LLC

# Pennsylvania Breach Of Personal Information Notification Act

- Enforcement:
  - A violation of this act shall be deemed to be an unfair or deceptive act or practice in violation of the Unfair Trade Practices and Consumer Protection Law.
  - The Office of Attorney General shall have exclusive authority to bring an action for a violation of this act.


© McNees Wallace & Nurick LLC

# Compare and Contrast: Enforcement

- Private cause of action for violation of breach notification laws:
  - 15 states provide a private cause of action
  - Most require the consumer have suffered an injury


© McNees Wallace & Nurick LLC

# Security Obligations for State Entities

- Entities who maintain, store, or manage computerized data on behalf of the Commonwealth that constitutes Personal Information must utilize encryption, or other appropriate security measures, to reasonably protect the transmission of Personal Information over the internet from being viewed or modified by an unauthorized third party.

- The same entities must develop and maintain:
  1. a policy to govern the encryption or other security measures; and
  2. a policy for data storage and retention.


© McNees Wallace & Nurick LLC

# Safe Harbors

- Encryption:
  - An entity must provide notice of the breach if encrypted information is accessed and acquired in an unencrypted form, if the security breach is linked to a breach of the security of the encryption or if the security breach involves a person with access to the encryption key.
- Employees
  - Good faith acquisition of personal information by an employee or agent of the entity for the purposes of the entity is not a breach of the security of the system if the personal information is not used for a purpose other than the lawful purpose of the entity and is not subject to further unauthorized disclosure.


© McNees Wallace & Nurick LLC

# Recent Trends in Cybersecurity

- RANSOMWARE – Widespread use, increasingly sophisticated
  - Municipalities are juicy targets – maintain PII, business interruption
- Stricter Regulation by States and Industry Regulators
- Cost of Cyber Liability Insurance and Difficulty Obtaining It
- Increased Demand for Boards and Governing Bodies to Become Involved in Cyber Risk Management
- Proliferation of Consumer Privacy Laws


© McNees Wallace & Nurick LLC

# Top 5 Data Breaches of 2023 (so far)

1. MOVEit: June 2023 (Mass hack of file transfer tool, 17.5million individuals impacted)
2. T-Mobile: January 2023 (hacker stole personal information from over 37 million customers)
3. Yum! Brands (KFC, Taco Bell, & Pizza Hut): April 2023 (hack compromised employee data)
4. ChatGPT: March 2023 (hack exposed user identifying information and partial payment information)
5. Chick-fil-A: March 2023 (breach of mobile app exposed customer personal information)


© McNees Wallace & Nurick LLC

# Questions?

**Sandy Garfinkel**
*Co-Chair, Privacy & Data Security Group*
McNees Wallace & Nurick LLC
sgarfinkel@mcneeslaw.com