Breach of Personal Information Notification Laws

NCRA Conference May-2024

Robert Gramola, Director of Administration
Pennsylvania Public Utility Commission

History of Breach Notification Laws

- California led the states in 2002 – making regulated entities and businesses responsible if a breach occurred
- This spread to all 50 states over the next 10 years
- Congress adopted Federal version in 2010
- 2022 – Federal law expanded as part of Cyber Incident Reporting and Critical Infrastructure Act to include breach of sensitive information held by government agency
- Most states are now expanding their laws to include responsibility by government agencies to coincide with the Federal expansion.

“Breach of the Security of the System”

- **Defined as:**

  The unauthorized access and acquisition of computerized data that materially compromises the security or confidentiality of personal information maintained by the agency as part of a database of personal information regarding multiple individuals

- **Causes OR reasonably believes has or will cause loss or injury to any individual.**

What Is Personal Information (PI)?

First name (or first initial) and last name with any of the following when the data IS NOT encrypted or redacted:

i. **Social Security Number**
ii. **Driver's license number or a State identification card**
iii. **Financial account number, credit or debit card number**
iv. **Medical information - individual's current or historical medical history, treatment or diagnosis.**
iv. **Health insurance information - individual's health insurance policy number or subscriber identification number**
v. **A username or e-mail address, in combination with a password or security question.**

Publicly available information that is lawfully made available to the general public from Federal, State, or local government records is not included. As per FOIA, Open Records, and Right to Know Laws

PAPUC

Laws in other States

- **ALL 50 states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have security breach notification laws.**
- **Require businesses to notify consumers if their Personal Information (PI) is breached.**
- **Most states – like Pennsylvania - have now expanded laws to make government agencies responsible when a breach of PI occurs.**
- **Has your Legislature expanded the law in your state to include a state agency or municipal government?**
- **In Pennsylvania – Act 151 effective May 2, 2023**

PAPUC

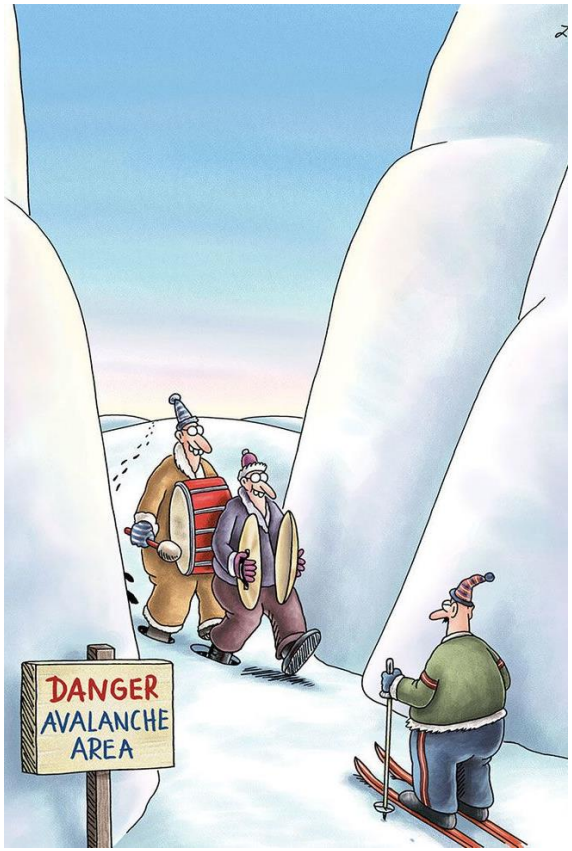
Who is Responsible for Breach of PI?

State agency - Any agency, board, commission, authority or department.

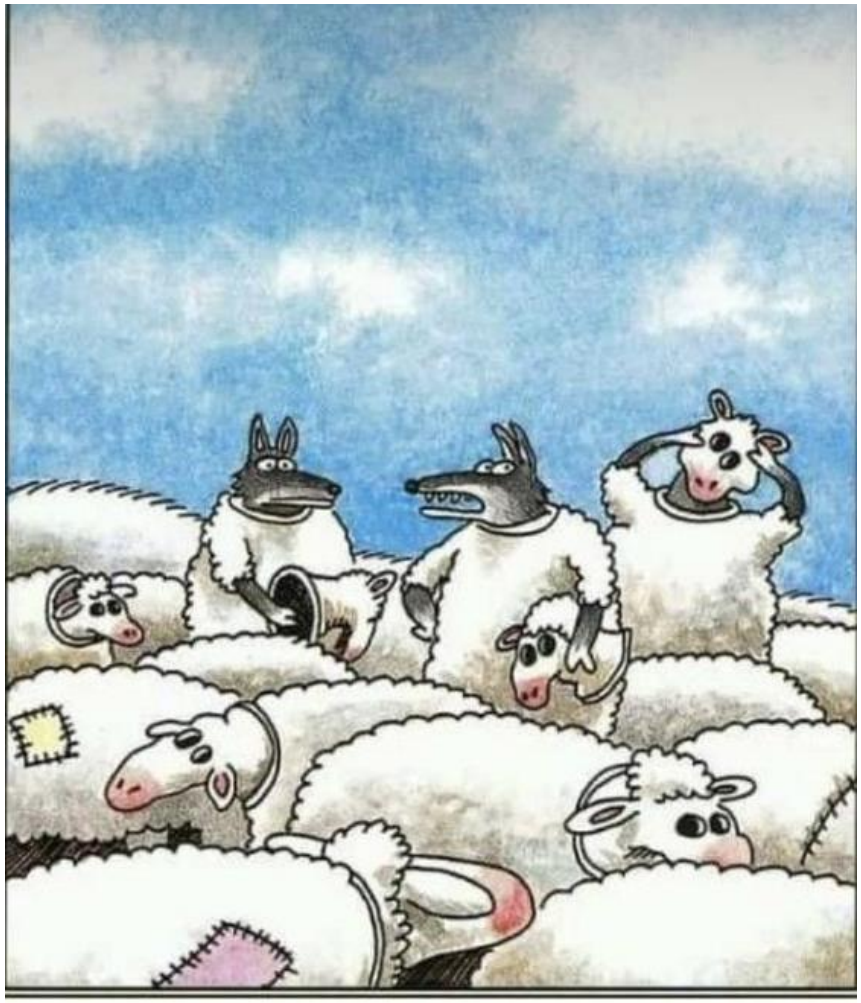
Entity - A State agency, a political subdivision or an individual or a business doing business in state where the law is enacted.

State agency contractor - A person, business, subcontractor or third-party subcontractor with contract that requires access to personal information.

Public school - any school district, intermediate unit, charter school, cyber charter school or area career and technical school.



Trigger for Notification of a Breach



"Wait a minute! Isn't anyone here a real sheep?"

WHAT HAS TO HAPPEN?

<u>Discovery</u> - Knowledge of OR Reasonable Suspicion Breach of the security of the system has occurred.

<u>Determination</u> - Verification OR Reasonable certainty Breach of the security of the system has occurred.

PAPUC

Notification Requirements

WHAT HAPPENS NEXT?

- **Agency MUST provide notice, without delay, to any individual that unencrypted and unredacted PI was or is reasonably believed to have been accessed and acquired by an unauthorized person.**

- **Agency vendor or contractor that maintains, stores, or manages computerized data shall provide notice of any breach upon discovery.**

- **Agency provides notice to more than 1,000 persons at one time and with out unreasonable delay to all consumer reporting agencies as per Fair Credit Reporting Act, of the timing, distribution and number of notices.**

Notification Requirements (cont.)

WHO HAS TO DO WHAT UNDER PENNSYLVANIA LAW?

- State agency MUST NOTIFY affected residents AND Office of Attorney General within 7 business days of determination – there was a breach!

- State agencies under Governor's jurisdiction MUST REPORT breach to Office of Administration within 3 business days of determination

- State agency contractor MUST NOTIFY State agency

- As soon as reasonably practical UPON discovery

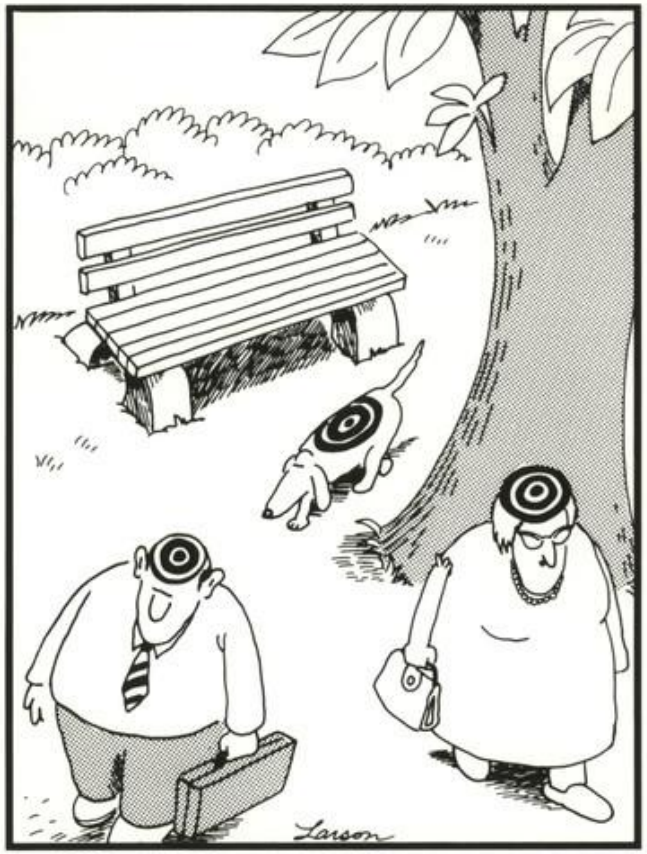
- But no later than the time period specified in the applicable terms of the contract.

- Local Government Entities (County, public school district, intermediate unit, charter school, cyber charter school or area career and technical school, or municipality) *MUST NOTIFY*
  - Affected residents within 7 business days of determination AND
  - District Attorney of the county where the breach of the security of the system occurred within 3 business days of determination

Notification Types

HOW DO WE TELL PEOPLE WHO ARE AFFECTED BY THE BREACH?

- **Written to last known home address of the individual.**
- **Telephonic notice, if the individual can be reasonably expected to receive it.**
- **E-mail notice, if agency has a previously used email address.**
- **Electronic notice, directing the affected individual to promptly change password or take other steps appropriate to protect the person's PI.**



How birds see the world.

Substitute Notification Types

HOW ELSE CAN WE NOTIFY THOSE AFFECTED?

Substitute notice, if the Agency demonstrates ONE of the following:

- **(A) Cost of providing notice would exceed $100,000 - OR**
- **(B) Affected class of subject persons notified exceeds 175,000 - OR**
- **(C) The agency does not have sufficient contact information.**

Substitute notice shall consist of ALL of the following:

- **(A) E-mail notice when agency has e-mail addresses for the persons affected.**
- **(B) Conspicuous posting on the agency's Internet website.**
- **(C) Notification to major Statewide media.**

Encryption & Storage Requirements

THE GOVERNMENT'S RESPONSIBILITY

- **Agencies that maintain, store, or manage computerized data (PI) SHALL:**
  - **Utilize encryption or other appropriate security measures, to reasonably protect the transmission of personal information over the Internet.**
  - **Develop and maintain a policy for proper encryption or other appropriate security measures for transmission of data**
  - **Develop a policy to govern reasonably proper storage of the personal information.**

Contractual Requirements

THIRD PARTY VENDORS AND CONTRACTORS

A state agency, after the effective date of this section, enters into a contract involving use of PI - Contractor SHALL ensure the contract includes provisions relating to the contractor's compliance.

Have a Plan

- The PA Commission had an internal Working Group to implement all the safeguards required by Act 151.
- PA New Law went into effect May 2, 2023.
- ENCRYPTION, ENCRYPTION…..AND MORE ENCRYPTION!
- Identify the bureaus or departments within your Commission where PI exists!
- Create specific policies and internal procedures.