Data Breach 101—How to Avoid a Virtual Catastrophe

Presented by
Eduard Goodman, J.D., LL.M., CIPP
Chief Privacy Officer

IDentityTheft 911
Protecting identities. Enhancing reputations.

In partnership with

THE HARTFORD

IDentity Theft 911 is solely responsible for the content of this webinar

Today's objectives:

- **Understand** what a data breach is from a regulatory perspective
- **Explore** how a data breach can occur
- **Recognize** your privacy and data risk exposures and liabilities
- **Identify** some basic ways to assess, reduce and manage the risks

IDentityTheft Protecting identities. Enhancing reputations. IDentity Theft 911® is solely responsible for the content of this webinar

What is a data breach?

Under state breach notification laws, businesses must notify customers, patients and/or employees if there has been a breach that exposes their Personally Identifiable Information (PII).

IDentityTheft 911
Protecting identities. Enhancing reputations.

What is a data breach?

Personally Identifiable Information (PII) includes …

- Social Security Numbers
- Driver's License/State Issued ID Numbers
- Payment Card Numbers
- Financial Account Numbers/Routing Info
- Health Information
- Biometric Data
- Secondary Identifiers (eg: mother's maiden name, date of birth, etc.)

IDentityTheft 911
Protecting identities. Enhancing reputations.

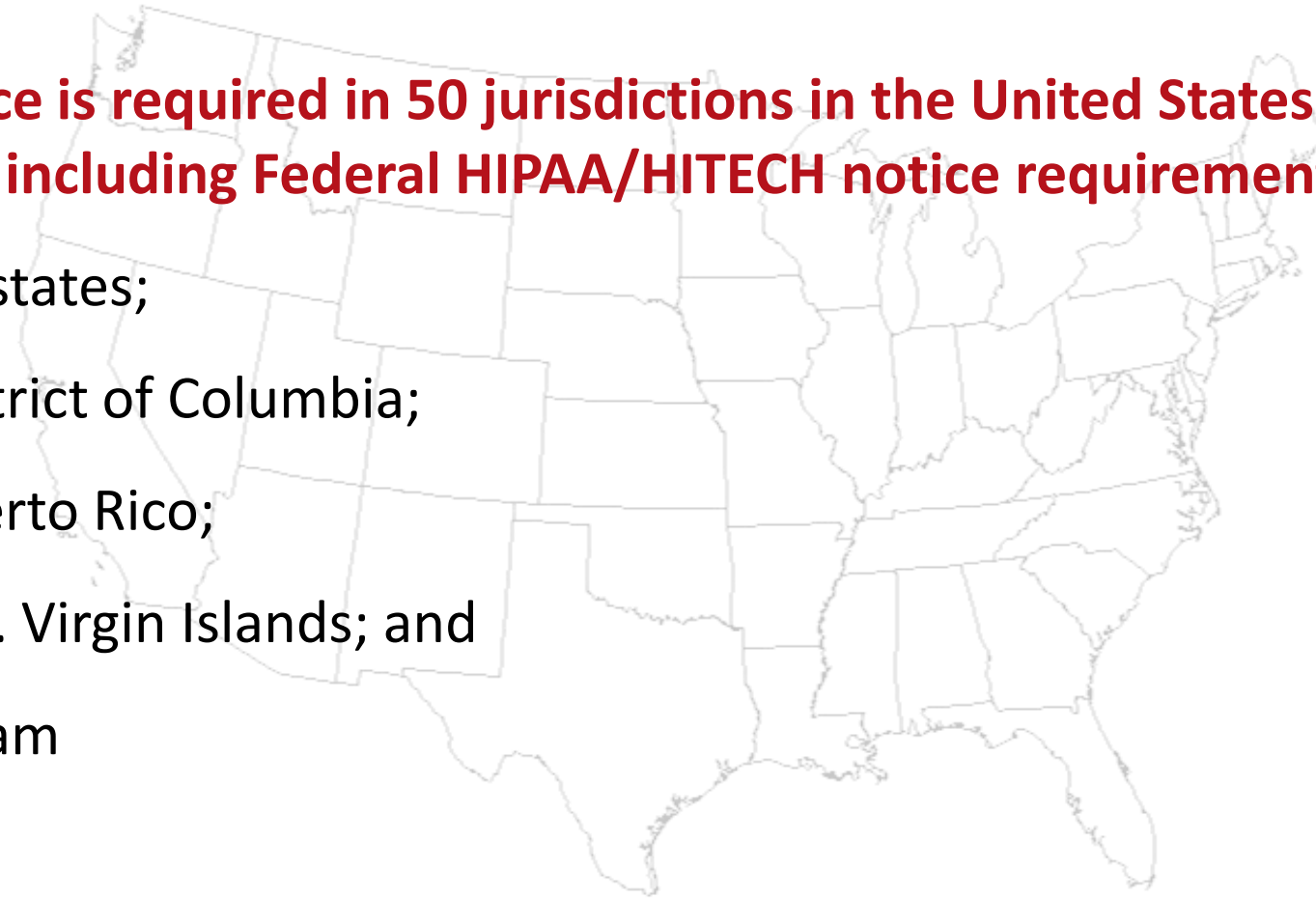
What is a data breach?

Depending upon the applicable state law, PII includes various forms of information/data. Examples include …

- Digital and hard copy data (or paper files);
- Encrypted/unencrypted data;
- Data lost by the business; and
- Data lost by a third party vendor

IDentityTheft 911
Protecting identities. Enhancing reputations.

What is a data breach?



Notice is required in 50 jurisdictions in the United States (51 laws including Federal HIPAA/HITECH notice requirements)

- 46 states;
- District of Columbia;
- Puerto Rico;
- U.S. Virgin Islands; and
- Guam

IDentityTheft 911
Protecting identities. Enhancing reputations.

What is a data breach?

The only states currently without a notification law are:

- Alabama;
- Kentucky;
- New Mexico; and
- South Dakota

IDentityTheft 911
Protecting identities. Enhancing reputations.

Common ways a data breach can happen

- Computer hacking
- Stolen or lost laptop or computer disks
- Stolen or lost paper documents / files
- Stolen credit card information
- Employee error or oversight

IDentityTheft 911
Protecting identities. Enhancing reputations.

What a data breach could mean for your business

- Loss of customer and/or employee trust
- Tarnished reputation
- Lost revenue

IDentityTheft 911
Protecting identities. Enhancing reputations.

State Data Breach Notification Laws

In addition to notification requirements, most states typically have (broad) language around the treatment, security and/or disposal of personal information wrapped up into their data breach notification regulations

IDentityTheft 911
Protecting identities. Enhancing reputations.

Self Regulatory Security Requirements

Payment Card Industry Data Security Standards (PCI-DSS)

Set of security requirements and standards promulgated by the payment card issuers (Visa, MasterCard, Discover, American Express, and JCB) regarding the storage and security of payment card-related data.

IDentityTheft 911
Protecting identities. Enhancing reputations.

Immediate To-Do List (Assess Exposure)

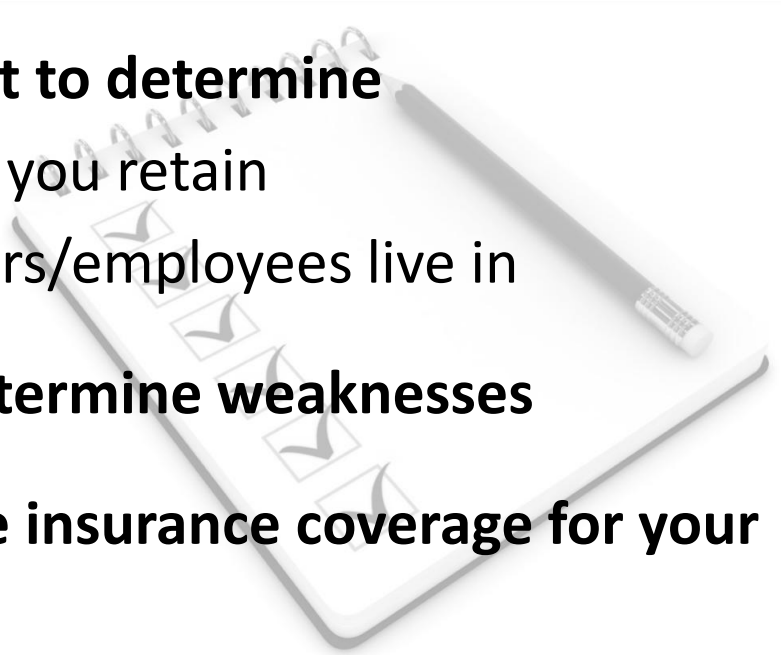
Consider the your business' "data footprint"

- What type of data is collected?
- From whom?
- From where?
- For what purpose?
- Who can access the data?
- Where is data stored, processed, etc?

IDentityTheft 911
Protecting identities. Enhancing reputations.

Immediate To-Do List

Assess and Cover Risk



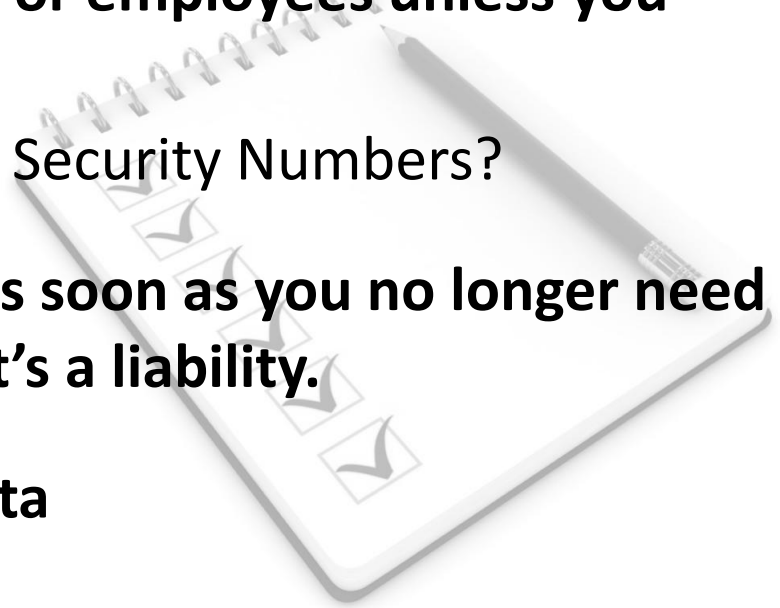
- **Complete high level “data” audit to determine**
  - Type of personal information you retain
  - What states do your customers/employees live in
- **Complete a Security audit to determine weaknesses**
- **Determine if you have adequate insurance coverage for your risk (eg: limits)**

IDentityTheft 911
Protecting identities. Enhancing reputations.

Immediate To-Do List

Help to reduce your risk or exposure

- **Don't collect data on customers or employees unless you need it**
  - Why are you collecting Social Security Numbers?
- **Get rid of any data you collect as soon as you no longer need it. It's toxic – it's not an asset; it's a liability.**
- **Encrypt any private personal data**



IDentityTheft 911
Protecting identities. Enhancing reputations.

Immediate To-Do List

Documentation / Programs

- Written Information Security Program
- Breach Response Plan
- Business Continuity Plan
- Data/Document Retention and Destruction Plan
- Data Security and Privacy Awareness Program

IDentityTheft 911
Protecting identities. Enhancing reputations.

Immediate To-Do List

Documentation / Programs

Develop a "privacy framework" for your business that fits from a:

- philosophical standpoint;
- business standpoint; and
- an operational standpoint

IDentityTheft 911
Protecting identities. Enhancing reputations.

For more data breach-related information …

Visit www.aahainsurance.org/ to get information on how to protect your practice with data breach insurance coverage and services. You will also receive a follow-up email with additional resources.

AAHA RECOMMENDED
The Standard of Veterinary Excellence

IDentityTheft 911
Protecting identities. Enhancing reputations.

IDentityTheft 911

Protecting identities. Enhancing reputations.

Thank you!

Eduard Goodman, J.D., LL.M., CIPP
Chief Privacy Officer
Scottsdale, Arizona

480.355.4940 direct
EGoodman@IDT911.com

In partnership with THE HARTFORD