A Day in the Life of a Breach

Ronald L. Chichester, JD, CFE, CISA
Ronald Chichester, P.C.

ISACA Greater Houston Area Chapter
One-Day, Two-Track Conference
August 17, 2015

Overview

- The Breach
- The Discovery
- The Consequences
- The Confession
- The Aftermath

Cast of Characters

- The Miscreant(s)
- The IT Person(s)
- Law Enforcement
- The Management
- The Lawyer(s)
- Agency Lawyer(s)
- Investors

The Lawyers

- Most lawyers are **not** technically trained
- They will ask seemingly odd questions
- Many questions will seem repetitive or redundant
- Questions are directed to satisfy disparate requirements from state/ federal governments

The Breach

- Let me count the ways...
  - Social engineering
  - Inside job
  - Lost laptop
  - Less protected (but trusted) contractor

The Discovery

- Need to find it
  - Monitoring
  - Customer complaint
  - Threat email
  - … (ad nauseam)
- Start the Clock

The Confession

- You have to help determine…
  - Whom to tell
  - What to tell them
  - When to tell them

Timeline

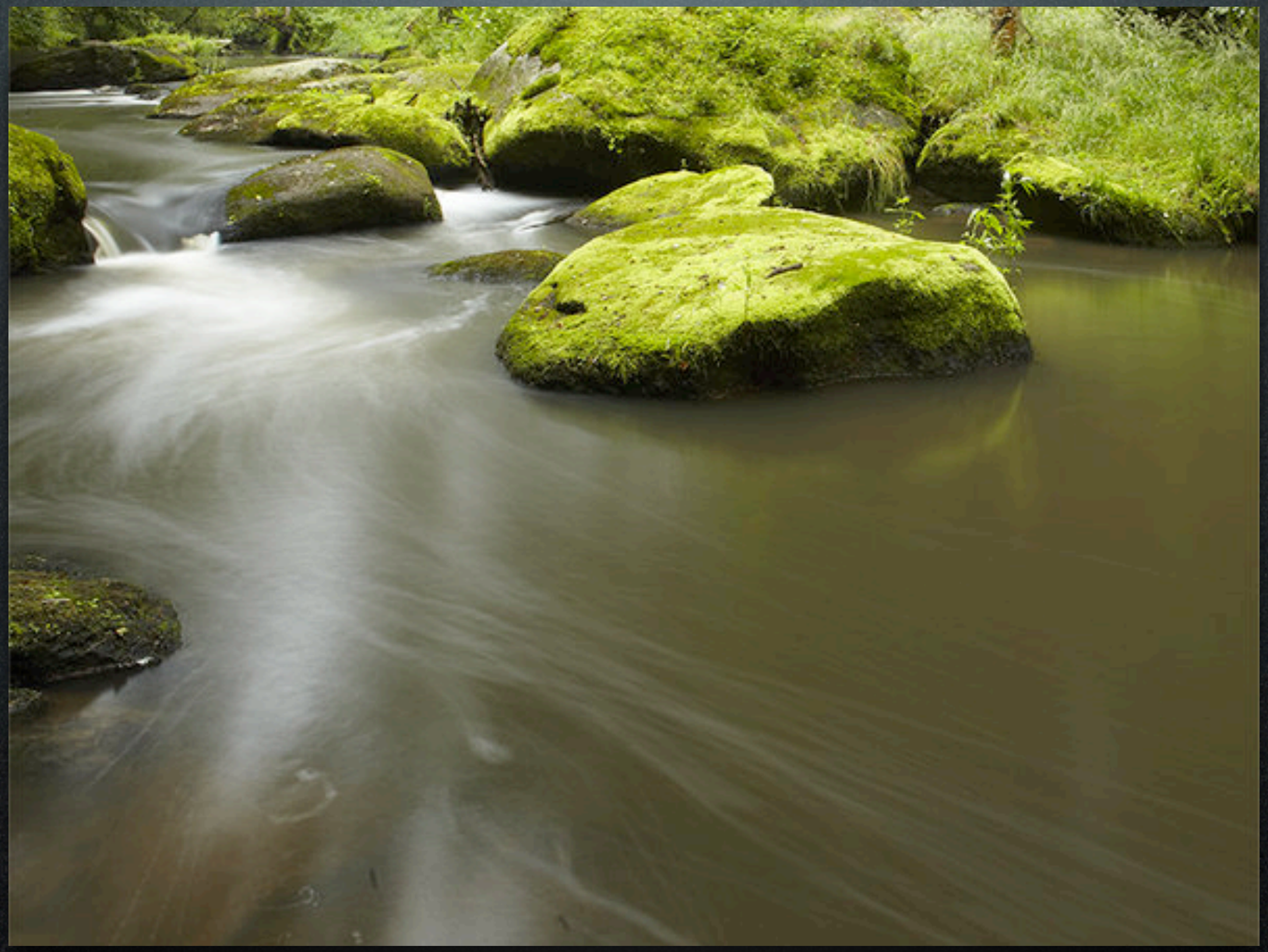
- Activate Response Team
- Call Insurance Agent
- Call the Attorney(s)
- Assign Coordinator
- Preserve the Evidence
- Call Law Enforcement
- Notify Government Agencies*
- Decide Who to Notify
- Offer Credit Monitoring
- Draft Press Release
- Draft FAQ's
- Notify Credit Card Companies

Timeline

- Activate Response Team
- Call Insurance Agent
- Call the Attorney(s)
- Assign Coordinator
- Preserve the Evidence
- Call Law Enforcement
- Notify Government Agencies
- Decide who to Notify
- Offer Credit Monitoring
- Draft Press Release
- Draft FAQ's
- Notify Credit Card Companies

The Clock is Ticking...

- Lots of laws (may) apply
- Some have short fuses
- You have to find out which states are affected
- You have to find out what kind of data was accessed or copied



What the law should be

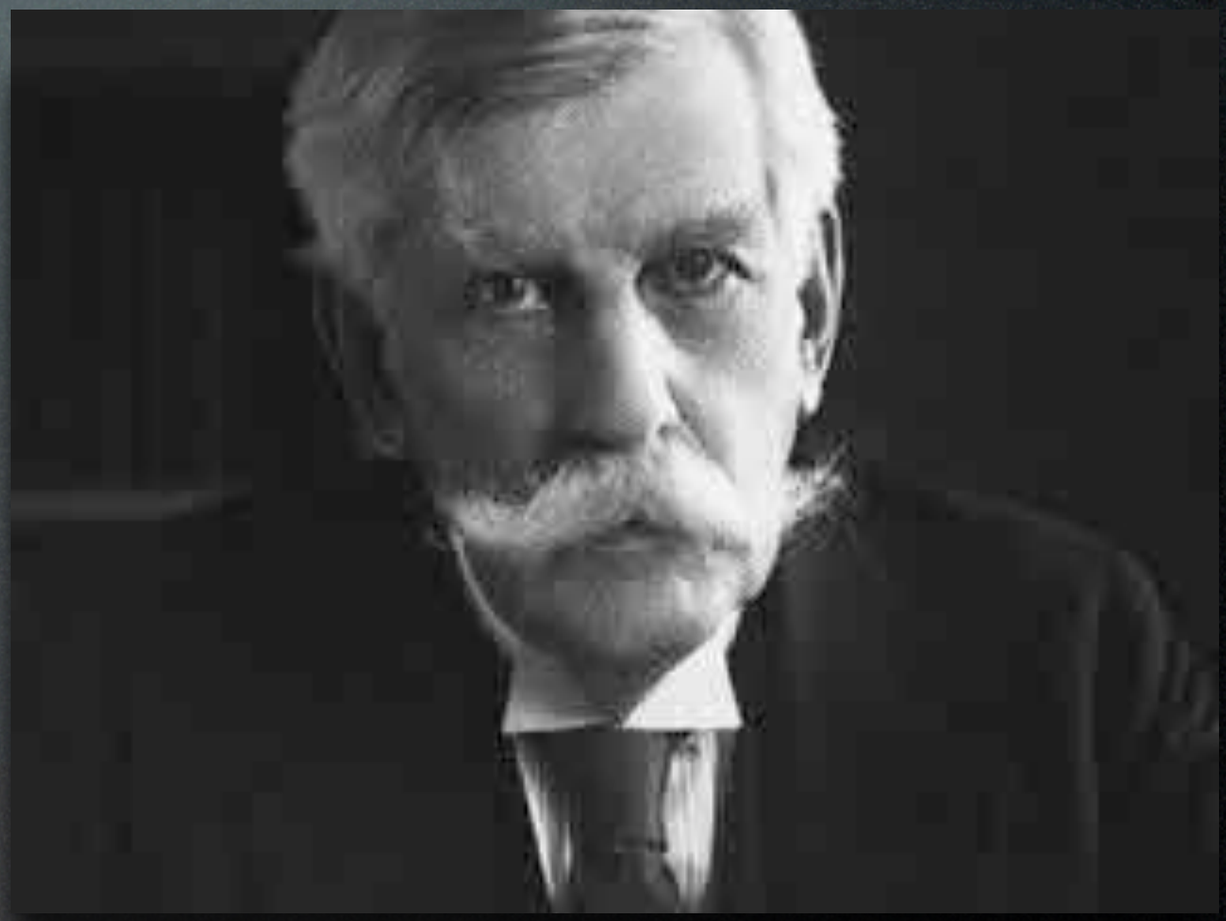
But the Feds...

... and so the states...

...gave us a mishmash

Oliver Wendell Holmes

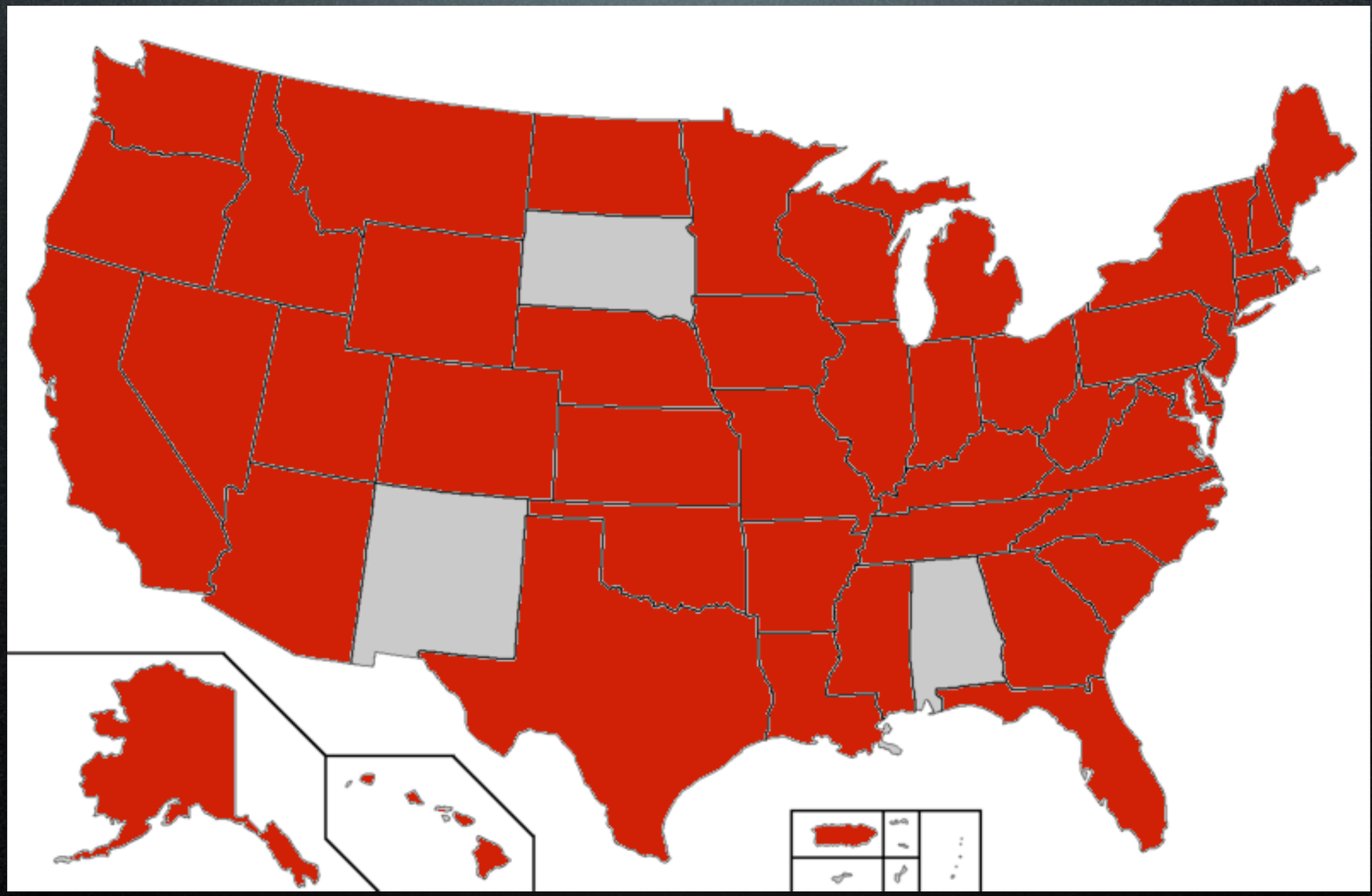
- The young man knows the rules...
- ... but the old man knows the exceptions



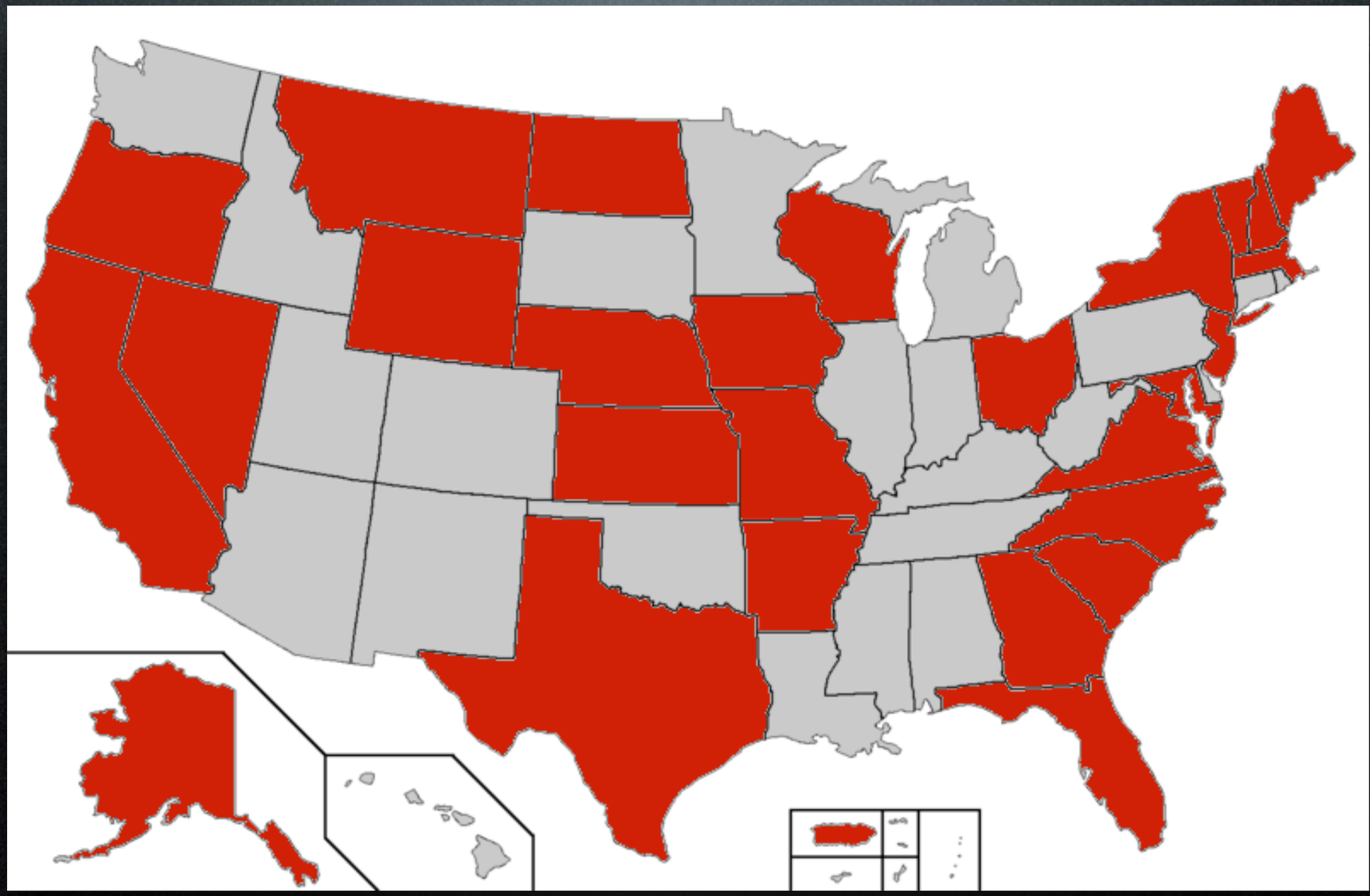
The Rules

- Personal Information
  - Common elements (First Name, Last Name, Gov't ID, Bank #, etc.)
- Breach of Security
  - The unlawful and unauthorized acquisition of personal information that compromises its security, confidentiality or integrity

The Exceptions



Safe Harbor for Encryption



Broader definition of “Personal Information”

Broader Definitions

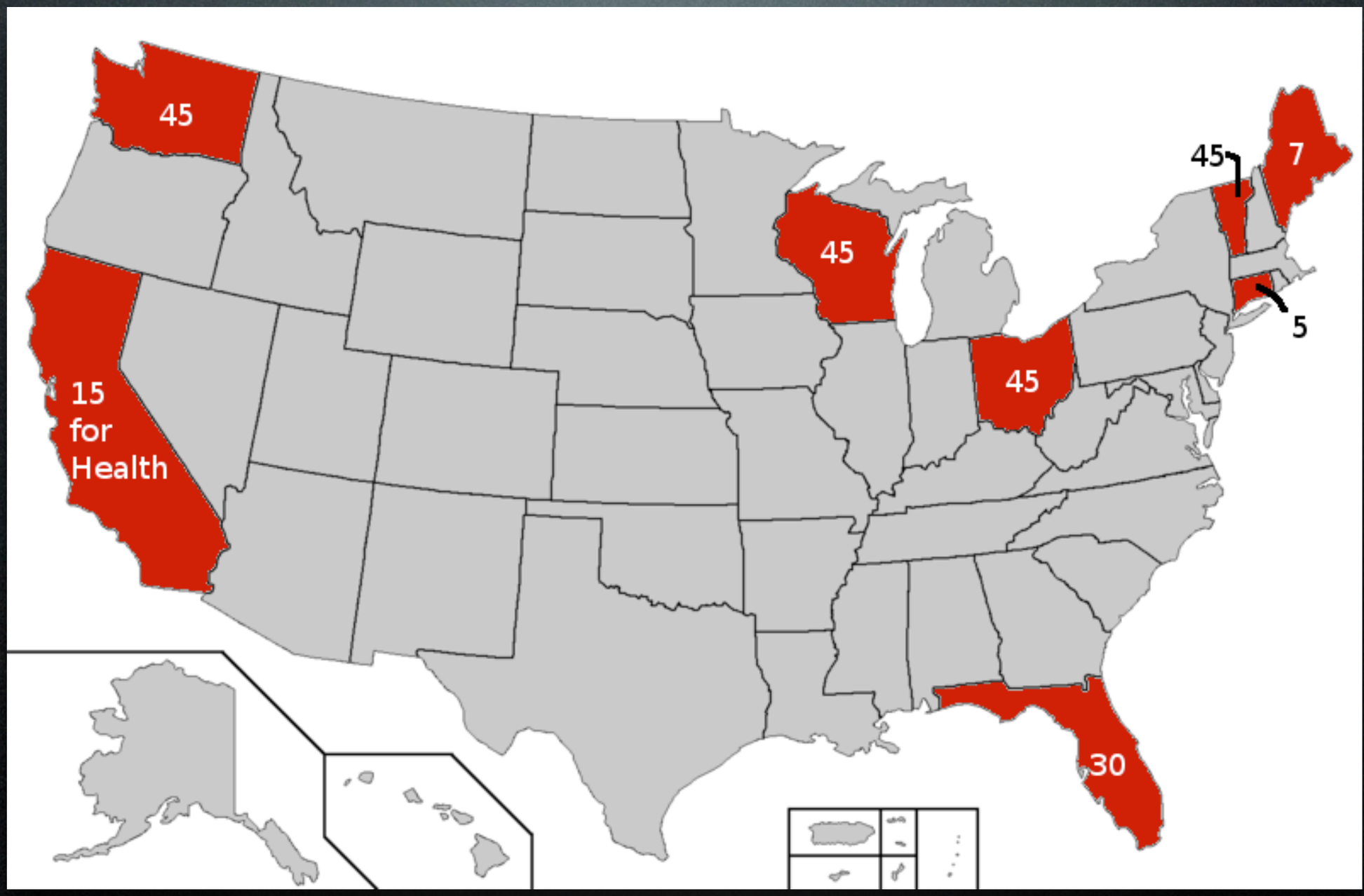
- Passwords to online accounts (CA, NV) (But NC expressly excludes)
- Taxpayer ID (MD, MT)
- Passwords to financial accounts (AK, FL, GA, IA, KS, ME, MA, MO, NY, ND, OR, SC, VT, WY, D.C., PR)

Broader Definitions

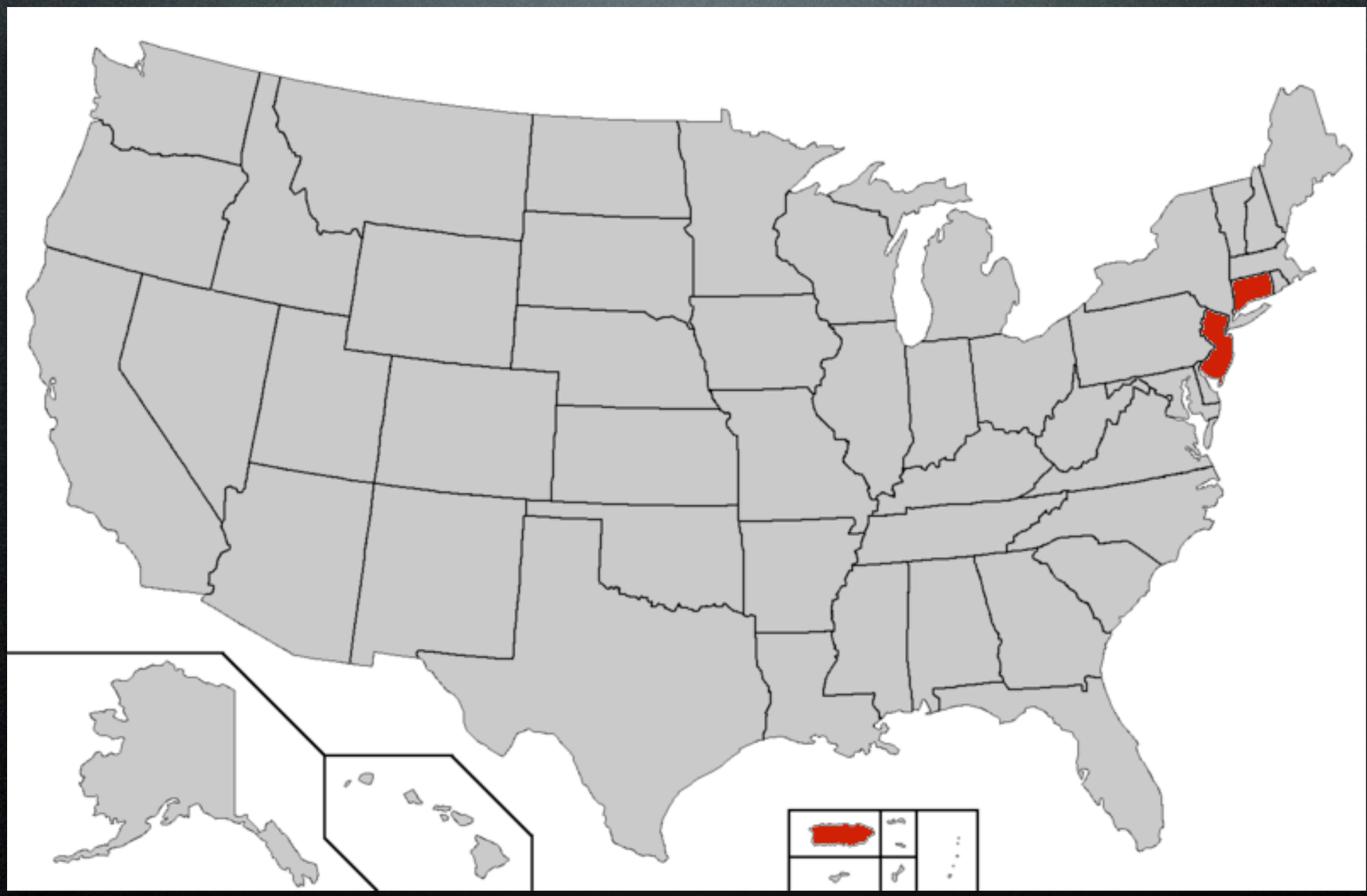
- Financial account info - with or without password (MA)
- Dissociated data -- if linked (NJ)
- Biometric data (NE, NC, VA)
- Digital/Electronic signature (ND)

Broader Definitions

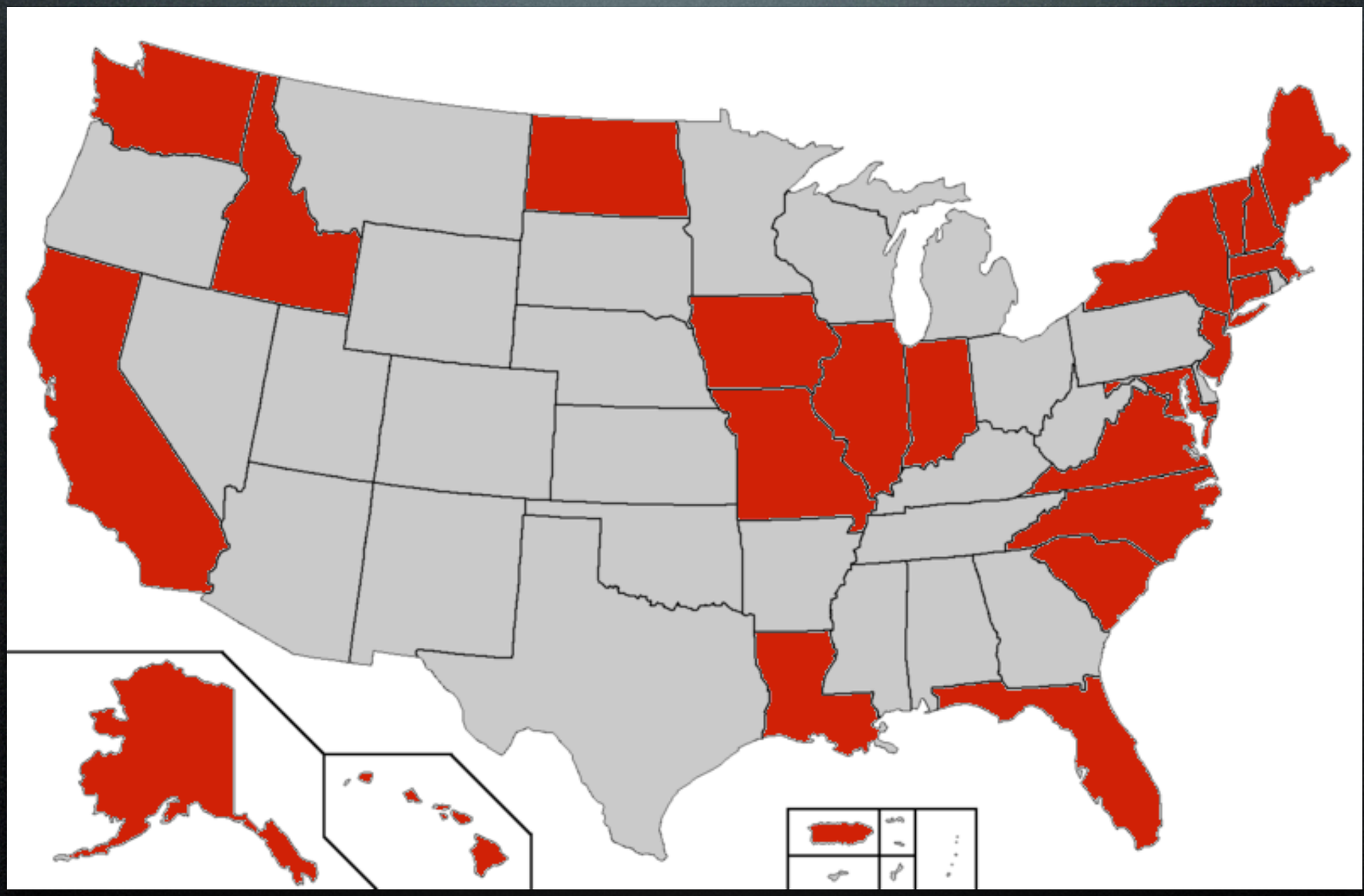
- Health ID for med account (NV, WY)
- Medical information & history (AR, CA, FL, MO, MT, NH, ND, TX, VA, WI (DNA only), WY, PR)



Short-fuse Timing for Notification



Trigger on Access (not Acquisition)



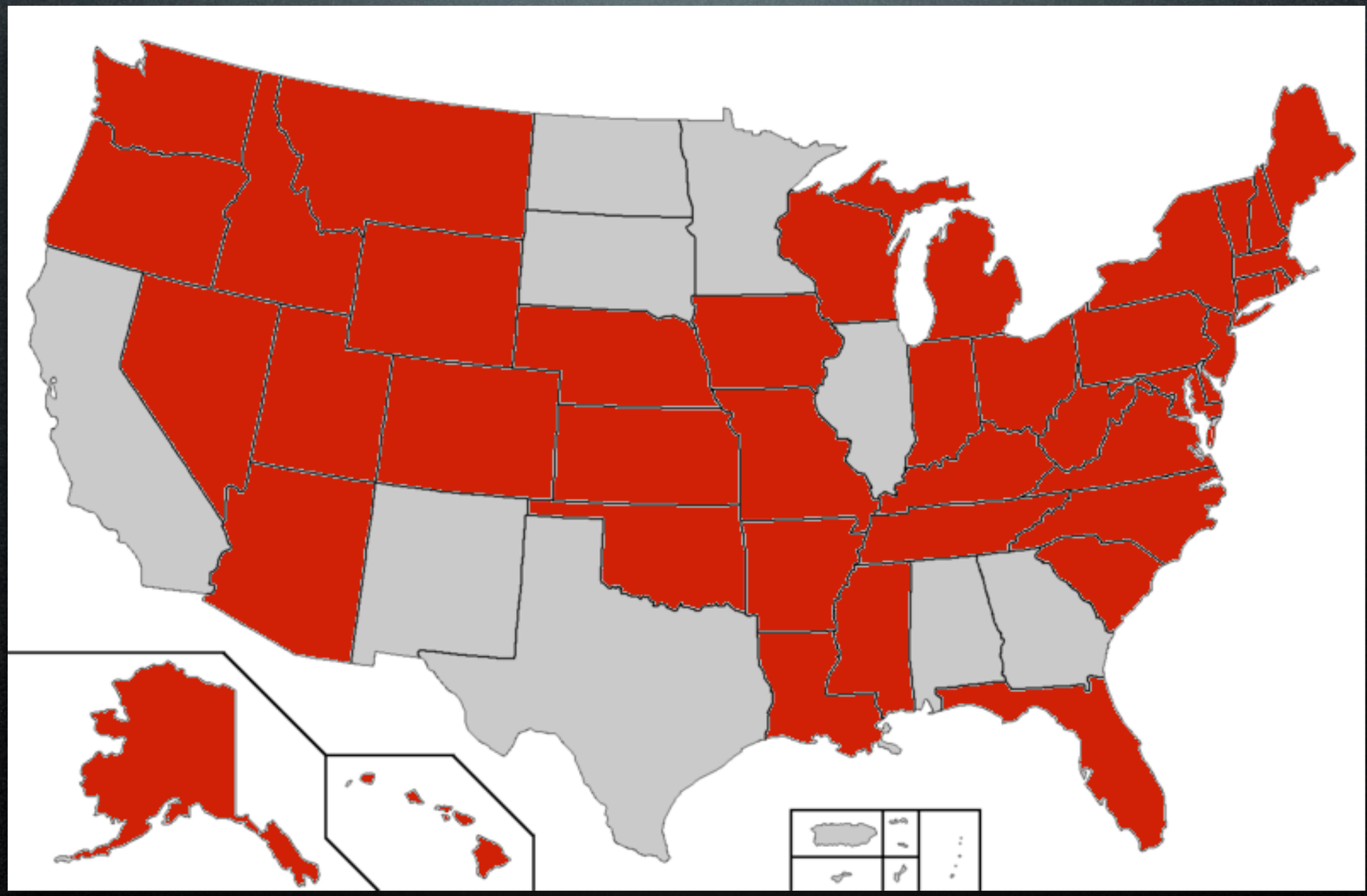
Notify the Attorney General or State Agency

Notify the State Gov't.

- Notify government if X customers are to be notified.
  - 1 or more - CT, IN, LA, MD, MA, MO, MT, NH, NJ, NY, NC, PR, VT
  - 250 or more - ND
  - 500 or more - CA, FL, IA, WA
  - 1000 or more - HI, MO, SC, VA

Notify the State Gov't.

- Notify gov't if gov't agency breached. (ID, IL)
- Notify gov't if the entity is governed by a professional or financial regulatory agency. (ME)
- Notify government that no notice required. (AK)



Risk of Harm Analysis

Risk of Harm Analysis

- Have to determine whether there was or is a reasonable likelihood that harm to the consumer has or will result. (AK, AR, CO, CT, DE, HI, ID*, IN, IA, KS, KY, LA, ME, MS, MO, NE, NC, OH, OK, OR, RI, SC, WA)
- Have to determine if there was material compromise (AZ, ID*, MT, NV, PA, TN, WI, WY)

Risk of Harm Analysis

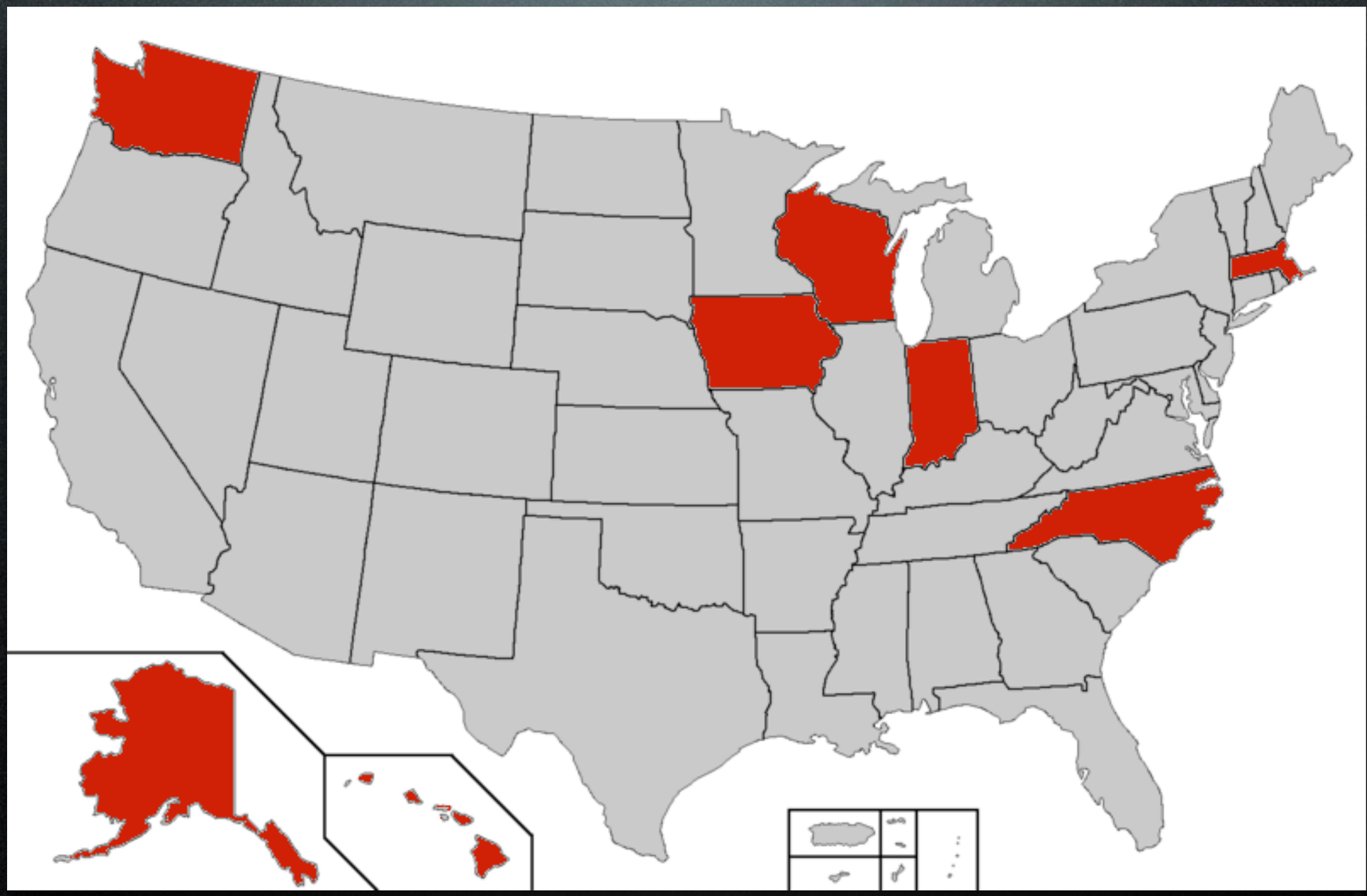
- Have to determine if the PI was not and will not be misused as a result of the breach. (MD)

- Have to determine if there is a substantial risk of identity theft (MA)

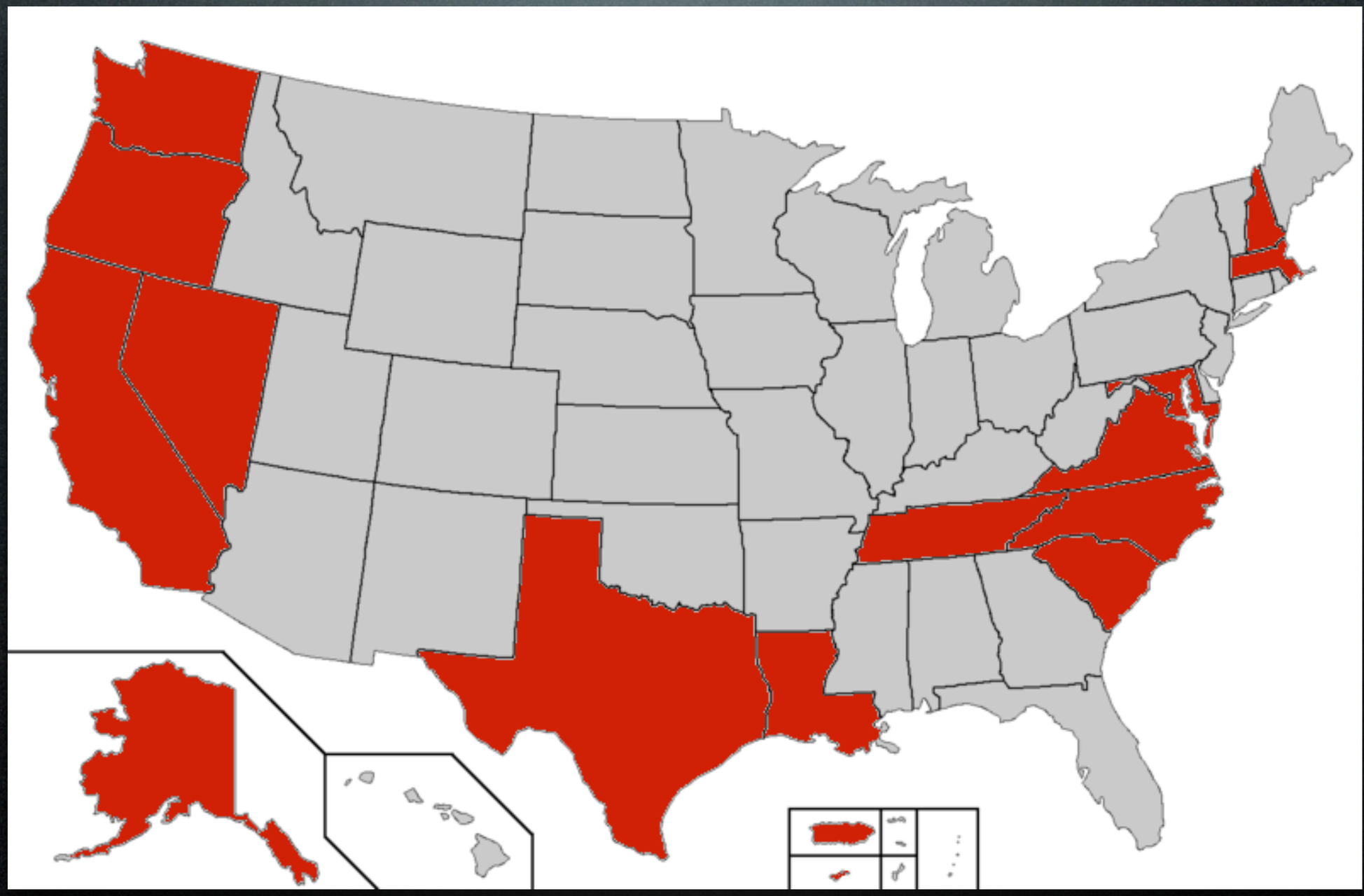
- Have to determine if the breach has or is likely (or will) to cause substantial loss or injury. (MI, VA, WV)

Risk of Harm Analysis

- Must determine if there was no misuse of data and not reasonably likely to occur. (NH, UT)
- Must determine if misuse is not reasonably possible. (NJ, VT)
- Must determine if there are "indications" of misuse. (NY)



Paper included in Breach Rubric



Private Cause of Action Permitted

Private Cause of Action

- Litigation Hold Notice must be imposed
  - In addition to law enforcement effort
  - Includes policies/procedures/audits
  - Emails, server logs
  - ...

Private Cause of Action

- Look forward to a second wave of lawyers
- Depositions/ Interrogatories/ Requests for Production
- Class Action or Disparate Jurisdiction
- Actual damages/court costs/attorneys fees

Federal Laws

- FTC Act
- Securities
- CFAA
- GLBA
- HIPAA
- COPPA
- Many more...

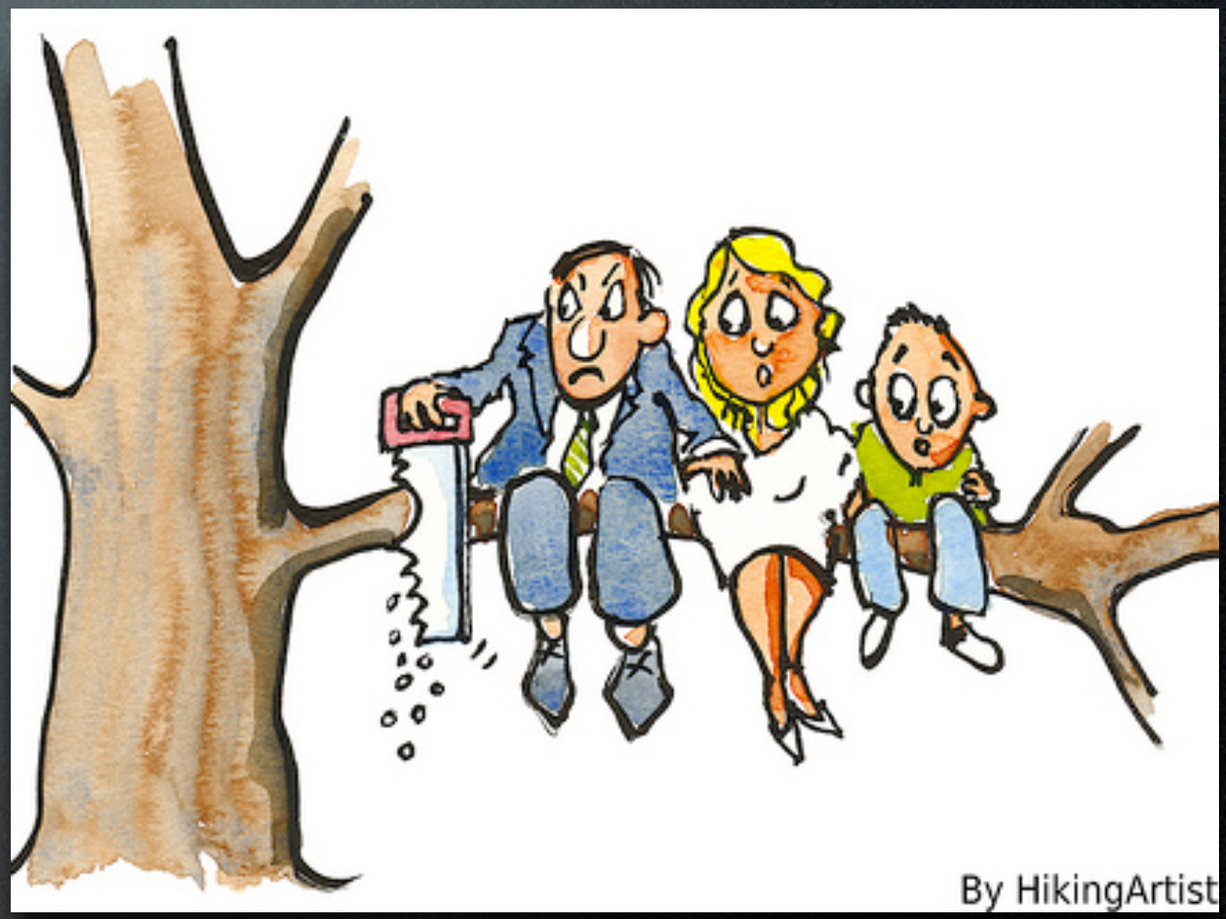
And lets not forget...

What to Expect

- Seemingly disparate questions directed to particular states
- You will need to make a distinction between access and acquisition
- You will need to supply a full list of what data types were compromised
- A short fuse

The Consequences

- Exposure to losses
- Lost sales/reputation
- 20 years of auditing
- FTC Action for Violations of Privacy Policy
- Disclosure in SEC 8-K and/or 10-K filings



The Aftermath

- In the past, there were few consequences
- Not so today
- This can get a CEO fired

Conclusions

- Watch what the FTC defines as “reasonable”
- Active monitoring
- Use encryption
- Rethink file indexing
- Broader scope of breach
- Have a plan ready in case you have a short fuse on notification

Questions?

Ronald Chichester, JD, CISA

713-302-1679

Ron@TexasComputerLaw.com