May 12, 2022

What Financial Sector Organizations Should Do to Address the New U.S. State Privacy Laws

Joy Chenault
CarMax

James Denvil
Hogan Lovells

Ron Whitworth
Truist

Roshni Patel
Hogan Lovells

Privacy+ Security Forum

State Privacy Law Framework

Privacy+ Security Forum

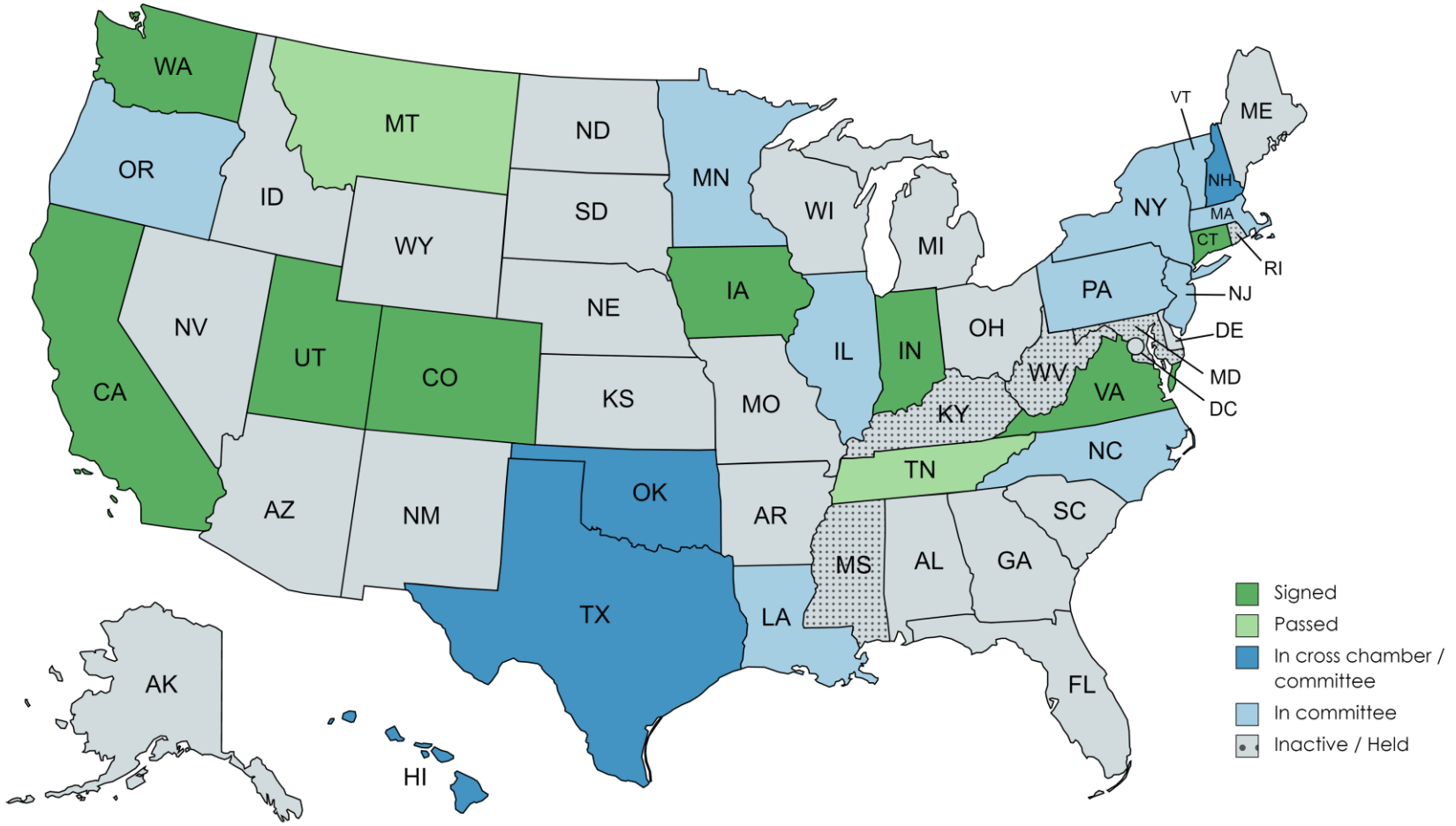
State Privacy Law Framework

- **The Original Five: Pre-2022 laws**
  - California, Colorado, Connecticut, Utah, Virginia
- **Newcomers in 2023**
  - Iowa, Indiana, Montana, Tennessee, Washington

State Privacy Law Framework

Privacy+ Security Forum

What Comes Next . . . ?



Key Compliance Obligations

Privacy+ Security Forum

Transparency

- Notice at collection
- Comprehensive privacy policy

Purpose Limitation

- Personal information can only be processed in accordance with notice
- New processing activities require notice, and in some cases consent

Consumer Rights

- Rights to know, access, and portability
- Deletion right
- Right to correct errors
- Opt-out rights for sales, targeted advertising, profiling

Data Processing Agreements

- Required service provider provisions
- Required for sales of personal information or sharing for targeted advertising

Key Compliance Obligations

Privacy+ Security Forum

Sensitive Personal Information

- Specific notice requirements
- Consent or an opt-out may be required

Data Protection Assessments

- Required if personal information processing presents a high risk to consumers

Service Provider Obligations

- Restrictions on use of personal information
- Flow-down of rights requests
- Assist in controller compliance

Training

- Employees must be trained on how to respond to rights requests

Washington's "My Health, My Data" Law

- Ostensibly a health privacy law, but any entity that collects "consumer health data" and does business in WA / targets products or services to WA consumers must comply
  - No revenue threshold or threshold for number of consumers whose data is processed
  - Not limited to entities in the health sector
- Applies to consumer health data
  - Broadly defined to mean "personal information that is linked or reasonably linkable to a consumer and that identifies the consumer's past, present or future physical or mental health status"
  - Includes, e.g., biometric data (broadly defined) and precise location data that could "reasonably indicate a consumer's attempt to acquire or receive health services or supplies"

Impact to Financial Institutions

Privacy+ Security Forum

Assessing Applicability

Full exemptions for financial institutions subject to GLBA	Exceptions to requirements for data subject to GLBA
Colorado	California
Connecticut	Colorado
Iowa	Connecticut
Indiana	Iowa
Montana	Indiana
Utah	Montana
Tennessee	Utah
Virginia	Tennessee
	Virginia
	Washington

Assessing Applicability

- **Personal information collected in the course of operating the business**
  - Categories of consumers:
    - Employees, contractors, applicants for employment, former employees
    - Representatives or agents of vendors
    - Business contacts or representatives of business partners
    - Shareholders, board members
  - Compliance considerations:
    - Privacy notices
    - Consumer rights

Assessing Applicability

- **Personal information collected in the course of offering commercial products**
  - Categories of consumers:
    - Employees or representatives of commercial borrowers, institutional investors, etc.
    - Individuals receiving products or services for commercial purposes
  - Compliance considerations:
    - Certain products and services may involve the processing of personal information covered by state law and GLBA-regulated data

Assessing Applicability

- **Personal information collected through websites or online services**
  - Categories of consumers:
    - Website visitors, targets of advertising on third-party websites
  - Compliance considerations:
    - In some cases, it may be impossible to tell if these individuals are "consumers" subject to GLBA / the GLBA exception applies
    - Selling personal information / targeted advertising compliance obligations