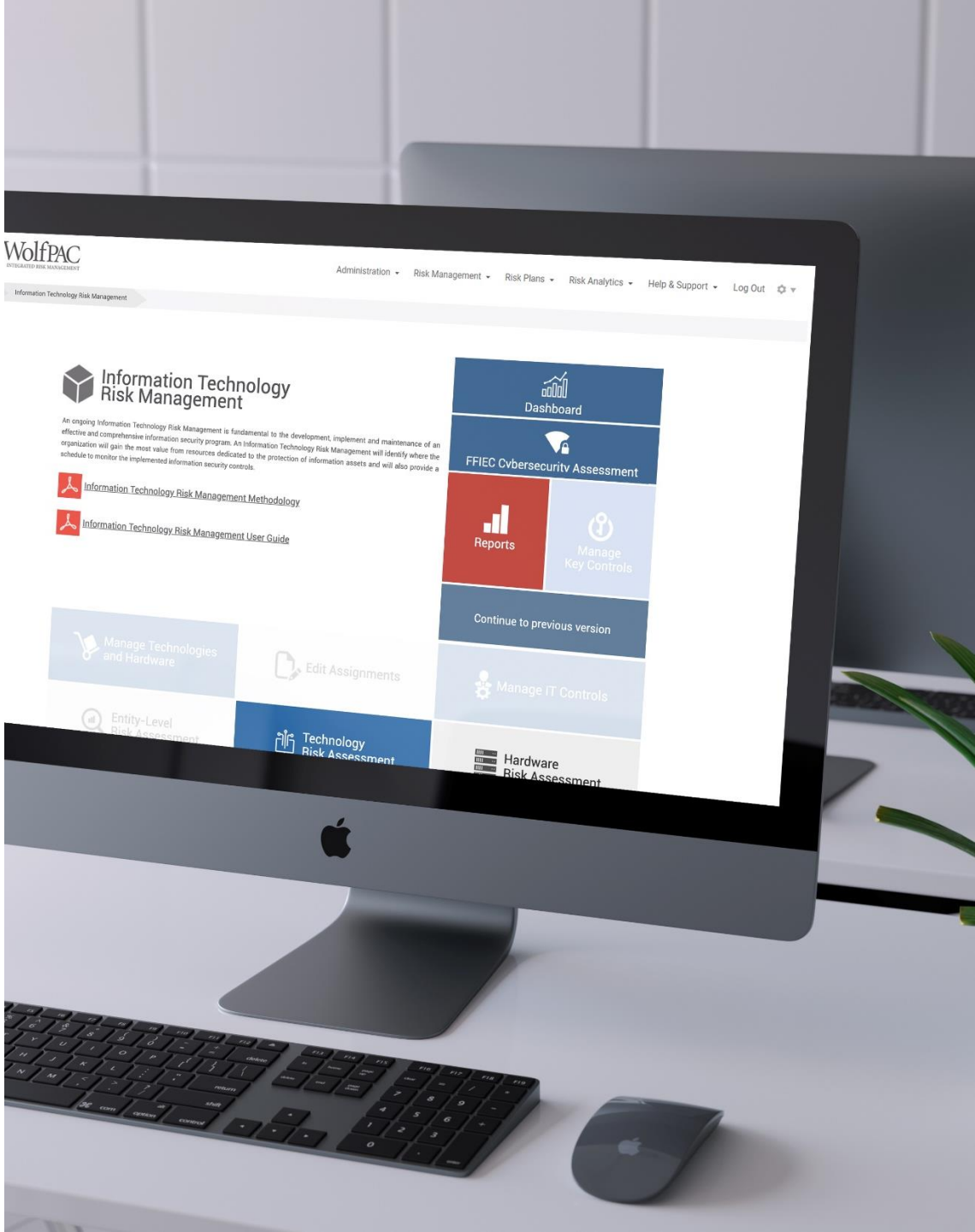
WolfPAC®
INTEGRATED RISK MANAGEMENT

Not Fully Exempt – California Privacy Law Compliance for Banks

Cynthia R. Boehmer, JD,CIPM
Manager



WOLF & COMPANY, P.C.

Presenter

CYNTHIA R. BOEHMER, JD, CIPM

Manager
Strategic Management Services
Direct: (617) 933-3340

cboehmer@wolfandco.com

Agenda

- Overview of current privacy laws
- Exemptions
  - Financial Institutions
- What do you need to comply with?
- California Privacy Protection Agency (CPPA)
- Enforcement Actions
- Other Privacy Laws
- Questions

Today's Privacy Picture

- California Consumer Privacy Act (CCPA) is currently in effect until January 1, 2023 at which time it is superseded by the California Privacy Rights Act (CPRA)
- Key Differences
  - Criteria for Qualifying as a Business
  - New Category of Sensitive Personal Information
  - New and Expanded Consumer Rights
  - Data minimization, purpose limitation and storage limitation
  - Expansion of actionable data in a breach
  - Creation of a Privacy Enforcement Authority

Covered Businesses

- Changes what is a covered business:
  - had $25M in annual gross revenues as of January 1 in the preceding calendar year; or
  - Buy, sell or share the personal information of 100,000 California consumers or households
  - Derives 50% or more of its revenues from selling or sharing personal information
- Sunsets the CCPA's exception for employee personal information and B2B personal information

Sensitive Personal Information (SPI)

- Newly created category that offers additional protections for consumer
  - **Government ID** — a consumer's Social Security, driver's license, state identification card, or passport number.
  - **Finances** — a consumer's account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account.
  - **Geolocation** — a consumer's precise geolocation.
  - **Race, religion and union membership** — a consumer's racial or ethnic origin, religious or philosophical beliefs, or union membership.
  - **Communications** — the contents of a consumer's private communications, unless the company is the intended recipient of the communication.
  - **Genetics** — a consumer's genetic data.
  - **Biometrics** — the processing of biometric information for the purpose of uniquely identifying a consumer.
  - **Health** — personal information collected and analyzed concerning a consumer's health.
  - **Sexual orientation** — personal information collected and analyzed concerning a consumer's sex life or sexual orientation.

Purpose Limitation Obligations

- Collection and Use of personal information is limited by the principles of necessity, proportionality and compatibility.
- A business's collection, use, retention and sharing of information must be:
  - Reasonably necessary and proportionate to achieve the purposes for which the PI was collected or for another disclosed purpose that is compatible with the context of the collection
  - Not further processed in a manner incompatible with those purposes

Consumer Rights

- CCPA and CPRA give consumers rights to:
  - Know what information is stored and access it any time
  - Right to have their data deleted upon request
  - Right to opt-out of sharing information
  - Consumer cannot be penalized for exercising rights
- Additional Rights under the CPRA:
  - Limit how sensitive personal information is used and disclosed
  - Request that any incorrect information be corrected
  - Opt-out of automated decision-making technology

Exemptions

- Medical information or Protected Health Information governed by California law, HIPAA or the “Common Rule” applicable to clinical trials;
- Personal information subject to the California Financial Information Privacy Act or the Gramm-Leach-Bliley Act (applicable to financial institutions)
- Personal information provided to or from consumer reporting agencies as governed by, and so long as maintained consistent with, the Fair Credit Reporting Act; and
- Personal information subject to protection under the Driver’s Privacy Protection Act

Exemptions – Financial Institutions

- Subject to the CCPA/CPRA, some (but not all) data may be exempt
- Does not apply to personal information collected, processed, sold or disclosed pursuant to the Gramm-Leach-Bliley Act (GLBA)
  - Under the CPRA it is “personal information collected, processed, sold, or disclosed ~~pursuant~~ ***subject*** to the federal Gramm-Leach-Bliley Act”
    - Will need further regulatory guidance on the impact of the change
- Fair Credit Reporting Act (FCRA) exemptions
  - All activity subject to FCRA is exempt

What is GLBA Nonpublic Personal Information?

- Any information an individual gives to get a financial product or service (for example, name, address, income, Social Security number, or other information on an application);

- Any information received about an individual from a transaction involving a financial product(s) or service(s)

- Any information obtained about an individual in connection with providing a financial product or service

Personal Information under CCPA

- Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier, IP address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers
- Customer records such as name, signature, social security number, physical characteristics or description, address, telephone number, passport number, driver's license or state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, or any other financial information, medical information, or health insurance information
- Characteristics of protected classifications under California or federal law such as race, ancestry, national origin, religion, age, mental and physical disability, sex, sexual orientation, gender identity, medical condition, genetic information, marital status, or military status
- Commercial information such as records of personal property, products or services purchased, or purchasing or consuming histories
- Biometric information
- Internet or other electronic network activity information such as browsing history, search history, or information regarding a consumer's interaction with a website, application, or advertisement
- Geolocation data
- Audio, electronic, visual, thermal, olfactory, or similar information
- Professional or employment-related information
- Education information not considered publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act
- Inferences that can create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, preferences, predispositions, behavior, attitudes, intelligence, abilities, or aptitudes

What does this mean for compliance?

- Personal Information not covered by GLBA
  - Information collected for marketing purposes
  - IP addresses, geolocation data, and/or cookies
    - Be careful of data collected through website visits

- Personal information of consumers not covered by GLBA
  - Those not obtaining a consumer financial product or service
    - Commercial or institutional customers
    - Employees or contractors
    - Service providers

No Exemptions

- Applicable to an individual's private right of action
- An individual is able to sue an organization if certain data elements of the organization unencrypted or non-redacted personal information was subject to a data breach if it was caused by a failure to implement appropriate and reasonable security practices and procedures
- This right extends to include GLBA data

What do you do?

- Have a process in place to identify what data is GLBA data and what is CCPA/CPRA data (i.e. through data mapping)
  - What is the purpose of data collected
  - Who are you collecting the data from?
- Reassess Privacy policies and practices
- Implement/update training programs
- Consider whether to expand program to include all data, even if exempt
- Process in place to respond to any consumers exercising rights and retain responses – especially if denial

California Privacy Protection Agency (CPPA)

- First privacy specific regulator in the U.S.
- Five-member board appointed by:
  - Governor (2 appointments including Chair)
  - Attorney General
  - Senate Rules Committee
  - Speaker of the Assembly
- Appointed in March 2021
- Serve at the pleasure of the appointing authority but no longer than 8 consecutive years
- Chief Privacy Auditor – power to audit business's compliance with CPRA

CPPA Responsibilities

- Rulemaking and enforcement authority
- Guidance to consumer on their rights
- Assistance and advice to legislature regarding privacy-related legislation
- Establishes mechanism for those doing business in California that do not qualify as a “business” to voluntarily certify that they are in compliance

CPPA – Enforcement Authority

- Authority to investigate at its discretion
- Initiate “probably cause proceedings” to evaluate whether an administrative hearing is needed
  - Must give notice 30 days prior to commencement of proceedings
- Enforcement through administrative actions
  - Attorney General retains civil enforcement
- Power to subpoena witnesses, compel testimony and take evidence
- Authority to order businesses to cease and desist from violations and pay administrative fines up to $2500 per violation ($7,500 for intentional violations or violations involving minors)

Increase Enforcement & Penalties

- Email address & password/security questions involved in data breach allows for a private right of action
- Increased fines for personal information involving minors
- Reduction in ability to cure
  - 30-day cure period for curing violations eliminated
  - 30-day cure period for curing data breaches preserved
    - Implementing and maintaining new security procedures after breach no longer constitutes a cure for that breach
  - Minimizes ability to reduce potential damages through remediate measures

Enforcement Actions

- Non-compliant service provider contracts
  - Did not prohibit service provider from retaining, using, or disclosing personal information received for any purpose other than performing the services specified in the contracts.
- Non-Compliant Privacy Policy
  - Did not provide notice of required CCPA consumer rights
- No “Do Not Sell My Personal Information” Link
  - Company sold information but did not include link on its website
- Untimely responses to CCPA Requests
  - Must respond within 45 days of requires (with 45 extension w/proper notice)
  - No response that request was received
- Charging Fees for CCPA requests
  - Not allowed to do so under the regulation

Other Considerations

- Need to comply with CCPA though December 31, 2022 as it applies to non-exempt data
- Privacy Policies must be updated every 12 months
- CPRA also imposes new requirements on third parties
- Look back period for CPRA begin January 1, 2022

Colorado Privacy Act (CPA)

- Applied to entities producing products and services for Colorado residents and
  - control or process personal data of at least 100,000 Colorado residents a year OR
  - control or process personal data of at least 25,000 consumers AND derive revenue or receive a discount on the price of goods or services from the sale of personal data
- Similar consumer rights as other privacy laws
- Exempt from the law - financial institutions and their affiliates along with data collected, processed, sold or disclosed pursuant to the Gramm-Leach-Bliley Act (GLBA)
- Non-profits are NOT exempt
- Enforcement through Colorado Attorney General and District Attorneys. No private right of action
- Effective Date: January 1, 2023

Thank You/ Q & A

CYNTHIA R. BOEHMER, JD, CIPM

Manager
Strategic Management Services
Direct: (617) 933-3340

cboehmer@wolfandco.com