AGENDA

• Background
• Key aspects
• Walking through provisions of CCPA
  • Business’s covered
  • Key definitions
  • Consumer rights
  • Penalties
    • Ability to cure
• Compliance
• This is an overview of the California Consumer Privacy Act of 2018. No information contained in this presentation is to be regarded as legal advice or direction.
BACKGROUND

California has a right to privacy

in the CA Constitution, 1972

In 1972, California voters amended the California Constitution to include the right of privacy among the “inalienable” rights of all people. The amendment established a legal and enforceable right of privacy for every Californian. Fundamental to this right of privacy is the ability of individuals to control the use, including the sale, of their personal information.

NorCal DA

AB375 Enacted in 2018, effective Jan 1, 2020

Grants a consumer a right to request a business to disclose the categories and specific pieces of personal information that it collects about the consumer, the categories of sources from which that information is collected, the business purposes for collecting or selling the information, and the categories of 3rd parties with which the information is shared.
IMPLICATIONS

- As goes California, so goes the country
  - Definite implications for other states and nationally
- Strong personal enforcement component
  - Individuals may bring enforcement actions
  - Class actions
    - Note, will discuss the opportunities to “cure”
FOR THOSE NOT IN COMPLIANCE

• Risks
  • Financial (of course)
    • Penalties, fines, litigation, mandated changes, revenue impact
  • Reputation
    • Damage to image and brand, impacting consumer sentiment
    • Impact on employees (Boeing)
  • Regulatory
    • Cost of non-compliance to be discussed later
QUESTION #1
KEY ASPECTS OF CCPA

• Transparency
• Disclosure
• Mechanism to object/opt out
WHAT IS THE CCPA

- Basics, what rights are being addressed:
  - The right to know about the personal information a business collects about them and how it is used and shared;
  - The right to delete personal information collected from them (with some exceptions);
  - The right to opt-out of the sale of their personal information; and
  - The right to non-discrimination for exercising their CCPA rights.

- Effective date
  - Jan 1, 2020
  - AG Directives July 1, 2020

- AG inputs
- Details later
WHO DOES THE CCPA IMPACT?

• Have a gross annual revenue of over $25 million;
• Buy, receive, or sell the personal information of 50,000 or more California residents, households, or devices; or
• Derive 50% or more of their annual revenue from selling California residents’ personal information.
• For now
  • Does not impact government agencies or non-profits
    • But ask yourself, where will it be in 5 years
    • Governments store enormous amounts of data
• NOTE:
  • These conditions are “OR”s not “AND”s
    • Any one triggers compliance
DEFINITIONS

• Consumer:
  • means a natural person who is a California resident, as defined in Section 17014 of Title 18 of the California Code of Regulations, as that section read on September 1, 2017, however identified, including by any unique identifier.

• Personal Information:
  • Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol (IP) address, email address, account name, social security number, driver’s license number, passport number, or other similar identifiers;
  • Any categories of personal information described in subdivision (e) of Section 1798.80.
  • Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer’s interaction with an Internet website, application, or advertisement;
  • Geolocation data, Biometric data
  • Audio, electronic, visual, thermal, olfactory, or similar information.
  • Professional or employment-related information
  • Education information, defined as information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act (20 U.S.C. section 1232g, 34 C.F.R. Part 99).
  • Inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer’s preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.
THE DEFINED RIGHTS FOR CONSUMERS
1798.100. (a) A consumer shall have the right to request that a business that collects a consumer’s personal information disclose to that consumer the categories and specific pieces of personal information the business has collected.

Categories include (From Attorney General’s Regulations)

- Specific pieces of personal information that a business has collected about the consumer;
- Categories of personal information it has collected about the consumer;
- Categories of sources from which the personal information is collected;
- Categories of personal information that the business sold or disclosed for a business purpose about the consumer;
- Categories of third parties to whom the personal information was sold or disclosed for a business purpose; and
- The business or commercial purpose for collecting or selling personal information.
1798.105. (a) A consumer shall have the right to request that a business delete any personal information about the consumer which the business has collected from the consumer.

- Business must disclose the consumer’s right to request deletion of their personal information
- A business that receives a verifiable request from a consumer to delete the consumer’s personal information pursuant to subdivision (a) of this section shall delete the consumer’s personal information from its records and direct any service providers to delete the consumer’s personal information from their records
  - Exclusions: legal obligation, transaction completion

Question:

- What about backups and archive?
RIGHT TO OPT OUT

• 999.306. Notice of Right to Opt-Out of Sale of Personal Information (a) Purpose and General Principles
  (1) The purpose of the notice of right to opt-out is to inform consumers of their right to direct a business that sells their personal information to stop selling their personal information.

• (2) The notice of right to opt-out shall be designed and presented in a way that is easy to read and understandable to consumers. The notice shall:
  • a. Use plain, straightforward language and avoid technical or legal jargon.
  • b. Use a format that draws the consumer’s attention to the notice and makes the notice readable, including on smaller screens, if applicable.
  • c. Be available in the languages in which the business in its ordinary course provides contracts, disclaimers, sale announcements, and other information to consumers in California.
A business that sells the personal information of consumers shall provide the notice of right to opt-out to consumers as follows:

1. A business shall post the notice of right to opt-out on the Internet webpage to which the consumer is directed after clicking on the “Do Not Sell My Personal Information” or “Do Not Sell My Info” link on the website homepage or the download or landing page of a mobile application.
**Important Privacy Choices**

MassMutual respects your privacy choices. If you have a relationship with a departing MassMutual financial professional, as described above, and you prefer that we do not share your personal information, such as information about your insurance policies or contracts held with us, with him or her under these circumstances, you can opt out of this sharing by directing us not to do so. If you wish to opt out of the sharing of your personal information with your departing MassMutual financial professional you may:

- Call us at (800) 272-2216

You may make this privacy choice and contact us at any time, however, if we do not hear from you we may share your information with your departing MassMutual financial professional as described above. If this is a joint account, if one joint owner tells us not to share information that choice will apply to the other owner or owners. If you have already told us your choice, there is no need to do so again.

If you have not purchased a product or service through a MassMutual financial professional or you do not have a relationship with a MassMutual financial professional, as described above, you do not need to contact us as we will not share your personal information other than as described in this notice.

Other than as described above, we will only share your personal information as permitted by law and, if the law requires us to obtain your consent or give you the opportunity to opt out of some types of sharing, we will do so before sharing the information.
AND HOW TO OPT BACK IN

• Consumers have the right to change their minds
  • Mechanism must be in place to opt back in
  • Should be part of overall policies
1798.125. (a) (1) A business shall not discriminate against a consumer because the consumer exercised any of the consumer’s rights under this title, including, but not limited to, by:

- Denying goods or services to the consumer.
- Charging different prices or rates for goods or services, including through the use of discounts or other benefits or imposing penalties.
- Providing a different level or quality of goods or services to the consumer, if the consumer exercises the consumer’s rights under this title.
- Suggesting that the consumer will receive a different price or rate for goods or services or a different level or quality of goods or services.
RIGHT TO NON-DISCRIMINATION, COMPLIANCE

• Policies and procedures
  • Review of policies, including pricing, to verify that consumer are not treated differently for invoking their rights under CCPA

• Notices
  • Informing consumers of the opportunity to receive incentives or other compensation for the sale of their personal information to third parties.

• Opt-in
  • Business may obtain consumer opt-in consent prior to enrolling in a financial incentive program
QUESTION #2
METHODS OF NOTICE

• **1798.100.** (a) A consumer shall have the right to request that a business that collects a consumer’s personal information disclose to that consumer the categories and specific pieces of personal information the business has collected.

• (b) A business that collects a consumer’s personal information shall, **at or before the point of collection**, inform consumers as to the categories of personal information to be collected and the purposes for which the categories of personal information shall be used.
At Massachusetts Mutual Life Insurance Company ("MassMutual") we recognize that our relationships with you are based on integrity and trust. As part of that trust relationship, we want you to understand that in order to provide our products and services to you, we must collect, use and share personal information about you. This Privacy Notice describes policies and practices about how we protect, collect and share personal information related to the products and services you receive from us, including life insurance, disability income insurance, long-term care insurance, and individual annuities. It also describes how you can limit some of that sharing.

We Protect Your Personal Information By:
- Using security measures that include physical, electronic and procedural safeguards to protect your personal information from unauthorized access or use in accordance with state and federal requirements.
- Training employees to safeguard personal information and restricting access to personal information to those employees who need it to perform their job functions.
- Contractually requiring business partners with whom we share your personal information to safeguard it and use it exclusively for the purpose for which it was shared.

Personal Information We May Collect:
The types of personal information we may collect depend on the type of product or service you have with us and may include:
- Information that you provide to us on applications or forms, during conversations with us or our representatives, or when you visit our website (for example, your name, address, Social Security number, date of birth, income, and assets, beneficiaries, and medical or health information).
- Information about your transactions with us and our affiliates, including your policy coverages, premiums, and payment history.
- Information from third parties such as consumer or other reporting agencies and medical or health care providers.
WEBSITE NOTICE, COMPLIANCE

• Organizations must disclose the following information in their online privacy policy — or on their website if they do not maintain a privacy policy — and update it at least once every 12 months:
  • A description of consumer rights under the CCPA and how to submit requests for information
  • A list of categories of personal information collected about consumers in the past 12 months
  • A list of categories of personal information sold about consumers in the past 12 months (if no personal information was sold, it must be stated)
  • A list of categories of personal information disclosed about consumers for a business purpose in the past 12 months (if no personal information was disclosed, it must be stated)
• Requests must be archived by the business for a minimum of 24 months

• Again, create and follow your policies, this is the best protection for compliance
How Aetna Uses and Discloses Personal Information

In order to provide you with insurance coverage, we need personal information about you, and we obtain that information from many different sources — particularly you, your employer or benefits plan sponsor if applicable, other insurers, HMOs or third-party administrators (TPAs), and health care providers. In administering your health benefits, we may use and disclose personal information about you in various ways, including:

Health Care Operations: We may use and disclose personal information during the course of running our health business — that is, during operational activities such as quality assessment and improvement; licensing; accreditation by independent organizations; performance measurement and outcomes assessment; health services research; and preventive health, disease management, case management and care coordination. For example, we may use the information to provide disease management programs for members with specific conditions, such as diabetes, asthma or heart failure. Other operational activities requiring use and disclosure include administration of reinsurance and stop loss, underwriting and rating; detection and investigation of fraud; administration of pharmaceutical

Payment: To help pay for your covered services, we may use and disclose personal information in a number of ways — in conducting utilization and medical necessity reviews; coordinating care; determining eligibility; determining formulary compliance; collecting premiums; calculating cost-sharing amounts; and responding to complaints, appeals and requests for external review. For example, we may use your medical history and other health information about you to decide whether a particular treatment is medically necessary and what the payment should be — and during the process, we may disclose information to your provider. We also mail Explanation of Benefits forms and other information

Your Legal Rights

The federal privacy regulations give you several rights regarding your health information. Here are some of your rights:

- You have the right to ask us to communicate with you in a certain form. For example, if you are covered as an adult dependent, you might ask us to send certain communications to another person or to your electronic or digital account. We will accommodate reasonable requests as long as you sign a written agreement specifying how, when, and to whom the communications will be directed.

- You have the right to ask us to restrict our use or disclosure of information in connection with health care operations, payment and treatment. You can ask us to restrict how we use or disclose your information to certain people or organizations, such as your employer. We will accommodate reasonable requests as long as you sign a written agreement specifying the restrictions.

- You have the right to request a copy of your health information. If you have an “designated record set” — medical records and other records maintained by us — you can ask us to provide copies or summaries of the information. Your request must be in writing and must include the reason for the request. If we deny your request, you will be notified in writing.

- You have the right to request an amendment of your health information. You can ask us to correct the information we maintain about you. Your request must be in writing and must include the information you want to amend and why the amendment is necessary.

- You have the right to request that we not use or disclose certain information to healthcare providers. You can request this as a condition of payment for a specified service. If you make such a request, we will comply with your request as long as we have not already disclosed the information to the healthcare provider.

- You have the right to request that we not disclose information to certain people or organizations. You can ask us to restrict how we use or disclose your information to certain people or organizations, such as your employer. We will accommodate reasonable requests as long as you sign a written agreement specifying how, when, and to whom the communications will be directed.

- You have the right to request that we not disclose information to certain people or organizations. You can ask us to restrict how we use or disclose your information to certain people or organizations, such as your employer. We will accommodate reasonable requests as long as you sign a written agreement specifying how, when, and to whom the communications will be directed.

- You have the right to request that we not disclose information to certain people or organizations. You can ask us to restrict how we use or disclose your information to certain people or organizations, such as your employer. We will accommodate reasonable requests as long as you sign a written agreement specifying how, when, and to whom the communications will be directed.

- You have the right to request that we not disclose information to certain people or organizations. You can ask us to restrict how we use or disclose your information to certain people or organizations, such as your employer. We will accommodate reasonable requests as long as you sign a written agreement specifying how, when, and to whom the communications will be directed.

- You have the right to request that we not disclose information to certain people or organizations. You can ask us to restrict how we use or disclose your information to certain people or organizations, such as your employer. We will accommodate reasonable requests as long as you sign a written agreement specifying how, when, and to whom the communications will be directed.

If you believe we have failed to provide these services or otherwise acted on a protected class noted above, you can also file a grievance with the Civil Rights Coordinator by contacting:

Civil Rights Coordinator,
P.O. Box 14462, Lexington, KY 40512 (CA HMO customers: PO Box CA 93779),
1-800-648-7817, TTY: 711,
Fax: 859-425-3379 (CA HMO customers: 860-262-7705), CRCoord

You can also file a civil rights complaint with the U.S. Department of Services, Office for Civil Rights Complaint Portal, available at https://ecrisportal.hhs.gov/ecrisportal/lobby.jsf, or at U.S. Department Services, 200 Independence Avenue SW., Room 509F, BBH Building 101, at 1-800-368-1019, 800-537-7697 (TDD).

Aetna is the brand name used for products and services provided by...
METHOD OF REQUESTS

• CCPA requires at least two methods available for consumers to exercise their rights under CCPA. At a minimum:
  • Toll free phone number
  • Website
  • Others are acceptable

• Timing
  • Disclosures must be made within 45 days from the request

• **Key point: Verifiable request**
  • “Verifiable consumer request” means a request that is made by a consumer, by a consumer on behalf of the consumer’s minor child, or by a natural person or a person registered with the Secretary of State, authorized by the consumer to act on the consumer’s behalf, and that the *business can reasonably verify*, pursuant to regulations adopted by the Attorney General pursuant to paragraph (7) of subdivision (a) of Section 1798.185 to be the consumer about whom the business has collected personal information.

  • Processes for verification must be in place and maintained for consumers to review
PENALTIES

• Attorney General Enforcement
  • Intentional violations: up $7500 per violation
  • Unintentional: up to $2500 per violation

• Private Action
  • Private plaintiffs may bring forward action for violation of the CCPA
  • Statutory damages from $100 to $750 per incident
    • Again, notice must be given and an opportunity to cure (next slide)
ABILITY TO CURE

• Companies have 30 days to cure after a notice
  • Prior to initiating any action against a business for statutory damages on an individual or class-wide basis, a consumer shall provide a business 30 days’ written notice identifying the specific provisions of this title the consumer alleges have been or are being violated. In the event a cure is possible, if within the 30 days the business actually cures the noticed violation and provides the consumer an express written statement that the violations have been cured and that no further violations shall occur, no action for individual statutory damages or class-wide statutory damages may be initiated against the business.
EXEMPTIONS

• Comply with federal, state, or local laws
• Comply with civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, or local authorities
• Cooperate with law enforcement agencies concerning conduct or activity that the business, service provider, or third party reasonably and in good faith believes may violate federal, state, or local law
• Exercise or defend legal claims
• Collect, use, retain, sell, or disclose consumer information that is de-identified or in the aggregate consumer information
• Collect or sell a consumer’s personal information if every aspect of that commercial conduct takes place wholly outside of California
MINORS AND LEGAL REQUIREMENTS

• For minors between 13 and 16, business must receive affirmative opt in consent
• For minors under 13, must receive consent from the parents or guardian of the minor, and also must be opt-in
• For firms that disregard the requirement, the CCPA deems that the business has actual knowledge of the minor’s age
  • Ignorance is no defense
COMPLIANCE

• Policies
  • Verify and update your privacy policies and notices to consumers. Make sure they are transparently conspicuous and easy to understand. Conform compliance with CCPA.
  • Data: make sure your data mapping and tracking are in place, so that your organization can easily comply with requests such as opt-out or deletion. Verify that you have a detailed understanding of your data collection processes, inventory and business uses.
  • Confirm cyber posture, perform risk assessments to identify risks, remediate, and protect PII.
  • Training: create and launch comprehensive training for employees to enact CCPA processes and policies.
BILL TEXT AND AG REGULATIONS

• CCPA bill text
  - https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375

• Attorney General’s regulations

• Comparison: GDPR vs CCPA
WRAP UP
• 1) Prior to tonight, have you read, with focus, any of the privacy disclosures sent to you by companies who send you privacy information?  (Y/N)

• 2) how long do you think it will take most of the rest of the states/federal government, to substantially implement CCPA in their jurisdictions?  A) 2 years  B) 5 years  C) 7 years  D) more than 7 years

• 3) How ready is your company, in general, for CCPA?  A) Less than 25% of the way there  B) 25 to 50% of the way there  C) 50 to 75% of the way there  d) over 75% of the way toward compliance