

JacksonLewis

California Consumer Privacy Act

Joe Lazzarotti, Esq., CIPP

Jackson Lewis P.C. • Berkeley Heights

Joseph.Lazzarotti@jacksonlewis.com • 908-795-5205

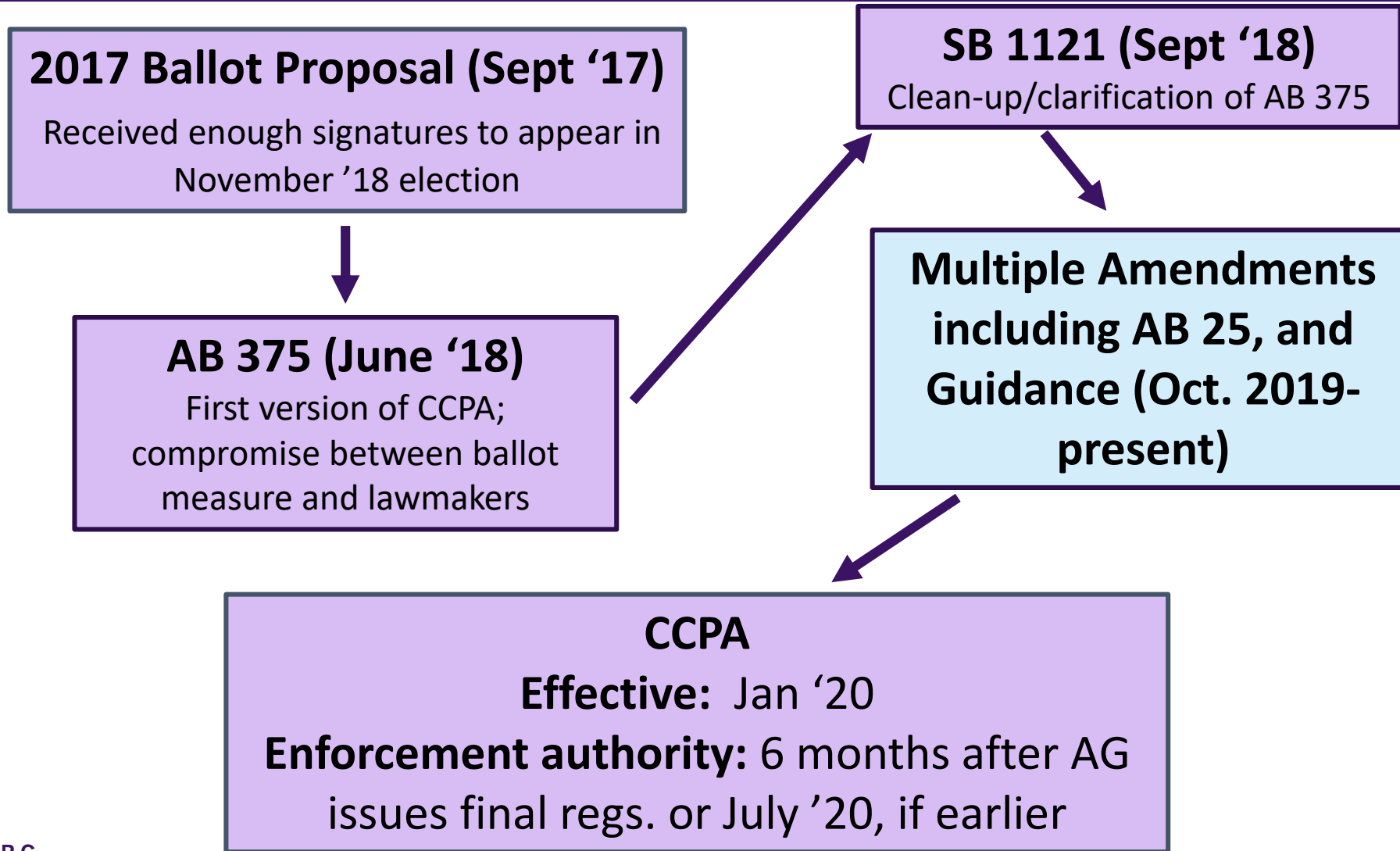
CCPA (January 1, 2020)

- Most expansive U.S. privacy law
 - Other states are considering/enacting similar laws (NJ, NY, MA)
 - Similar to GDPR (May 2018)
- Climate
 - Sweeping global changes to privacy and security
 - Growing appetite for more data

CCPA (January 1, 2020)

- Focus
 - Individuals rights (notice, access, deletion, opt-out)
 - Data security
- Penalties
 - Enforcement by the AG (up to \$7,500/violation)
 - Law currently allows for a 30-day cure period
- Private Right of Action
 - Reasonable safeguards
 - Statutory damages \$100 to \$750

How Did We Get Here?





Applies to the personal information of California consumers

Consumer: natural person, CA resident

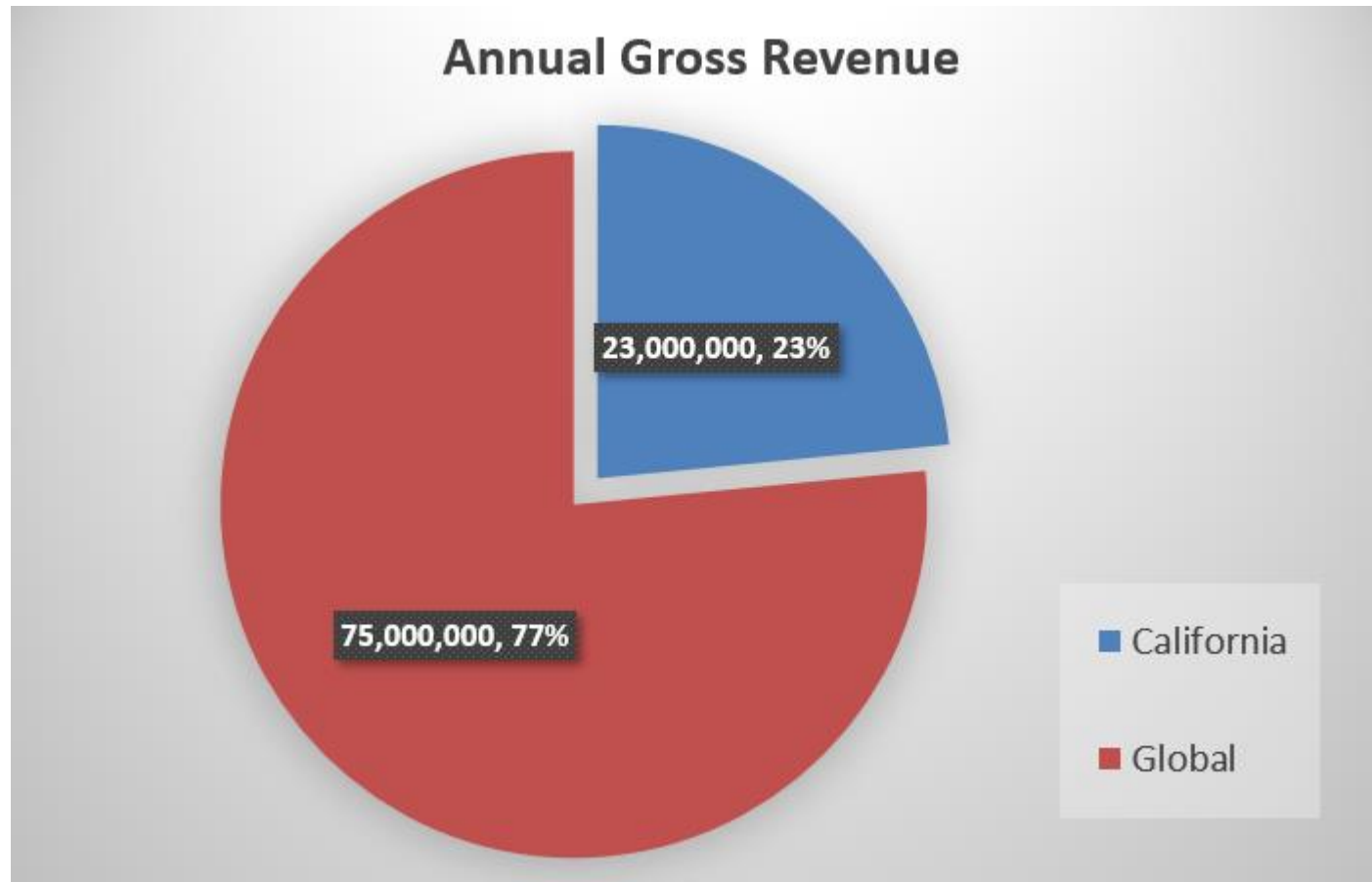


For-profit business, doing business in CA, that collects and controls personal information, and has any of following:

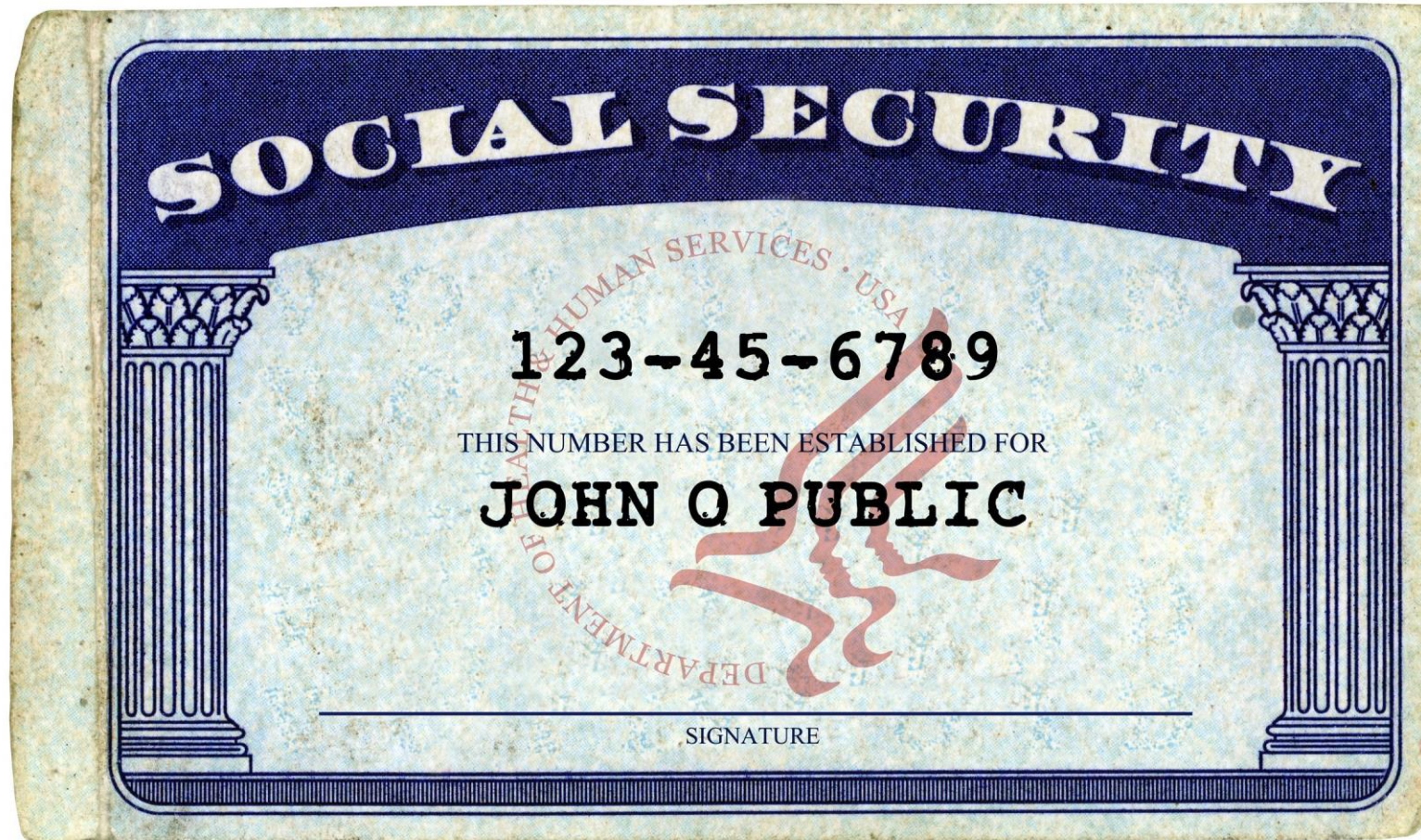
- Annual gross revenue greater than \$25M
- Annually buys, receives for commercial purposes, sells or shares personal information about more than 50,000 consumers, households or devices
- Derives 50% or more of annual revenue from selling consumer's personal information

CCPA Open Questions/Issues

\$25M or more annual gross revenue



Personal Information Under CCPA



Personal Information Under CCPA

Information that can identify, relate to, describe, or reasonably capable of being associated with or linked (directly or indirectly) to a particular individual or household.

- Identifiers
 - Name and address (post, email, IP)
 - **SSN, Driver's license**
 - Financial information
- Specific categories (1798.80(e))
- Protected classifications (CA, federal law)
- Commercial information
- Biometric information
- Internet/network activity
- Geolocation data
- Audio, electronic or visual information
- Professional/Employment
- Education
- **Inferences for profiling**



CCPA Exceptions?

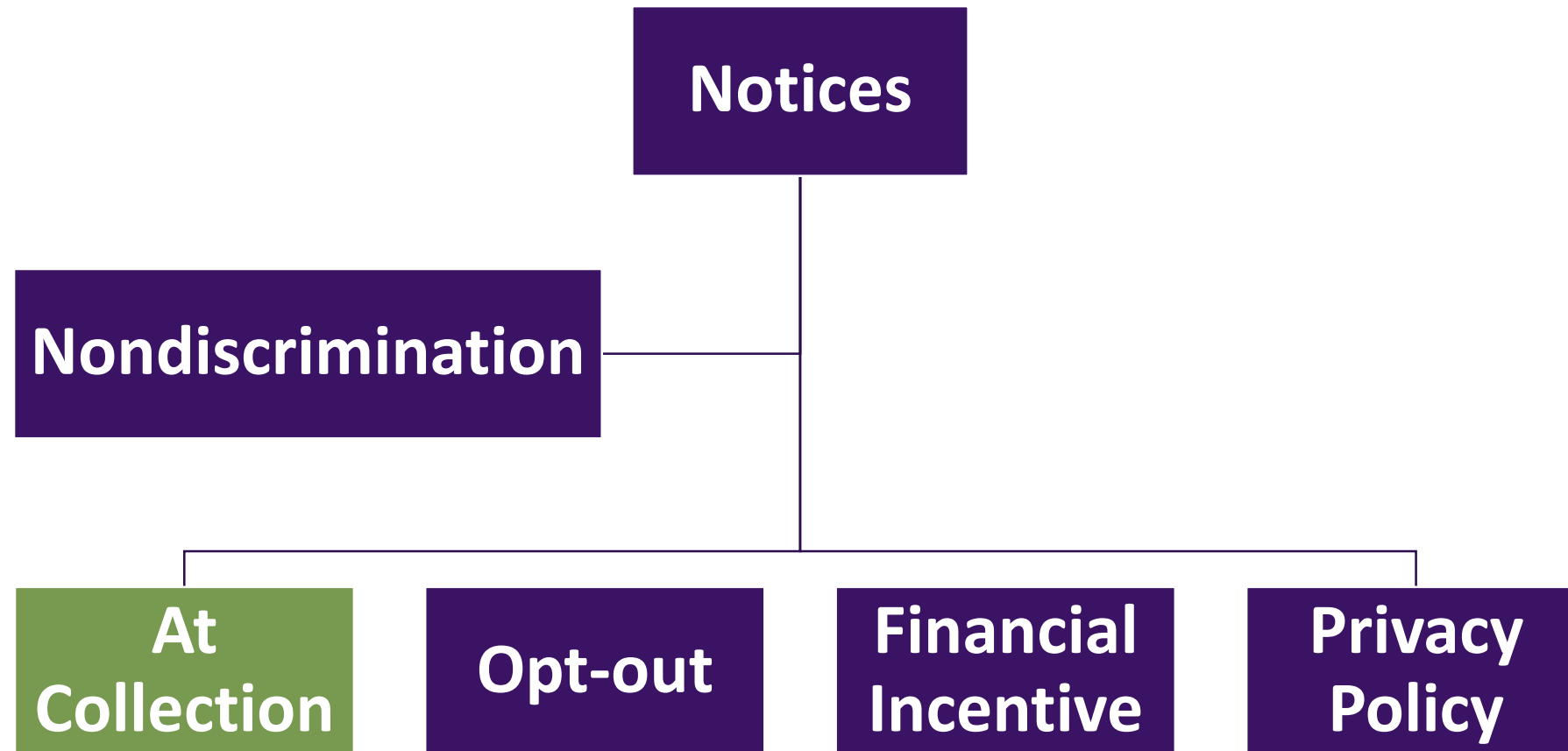
Employment data? – Yes, but. (AB 25)

**Business contacts? – Yes, but.
(AB 1355)**

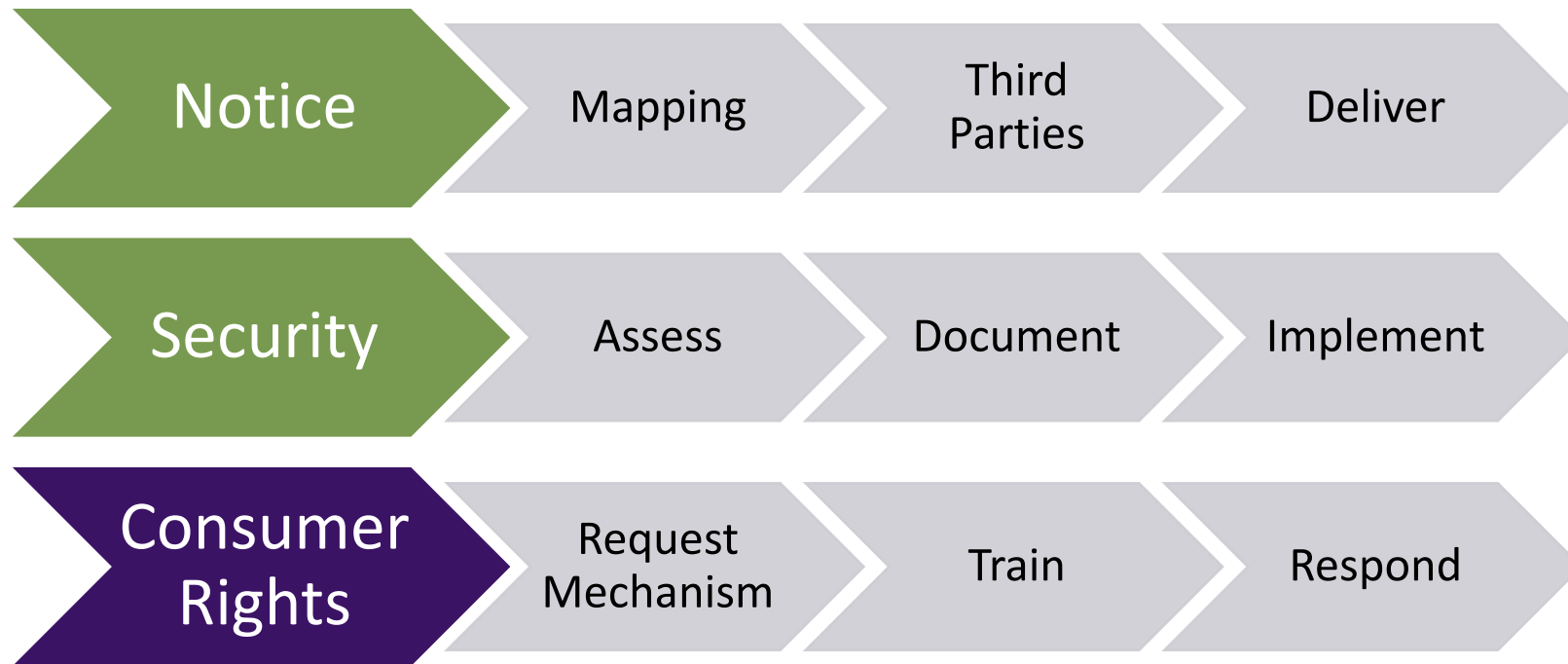
CCPA for Employers

- **AB 25 – The CCPA does not (for the next 12 months) apply to**
 - PI collected by a business about a natural person in the course of the natural person acting as a job applicant, employee, owner, director, officer, medical staff member, or contractor of that business **to the extent** that the PI is collected and used solely within the context of such natural person's role or former role with that business.
 - Similar exclusions for
 - i. emergency contact information of such persons, and
 - ii. PI that is necessary for the business to retain to administer benefits for another natural person relating to such natural person to the extent that the personal information is collected and used solely within the context of administering those benefits.
- **EXCEPT**

Rights Under CCPA



Obligations Under CCPA



Notice at Collection

- **Timing**
 - At or before collection
- **Content**
 - Categories of Personal Information
 - For each category, the purposes that each category will be used
 - “Do Not Sell My Personal Information” or similar link, if required.
 - Link to the business’s privacy policy.
- **Format**
 - Plain language
 - Draw attention to the notice, readable, including on smaller screens, if applicable
 - Be available in languages business uses in other communications
 - Be accessible to consumers with disabilities. At a minimum, provide information on how a consumer with a disability may access the notice in an alternative format.

Notice at Collection

Format (ctd.)

- Be visible or accessible where consumers will see it before any PI is collected.

Effect of Notice

- No notice, no collection of PI
- No collection of PI other than disclosed in the notice.
- No use of PI for any purpose other than disclosed in the notice.

Delivery

- For online collection, via a link to the section of the business's privacy policy.
- Other options – hand delivery, signage, email, with application.
- If business does not collect PI directly, it does not need to provide a notice at collection

Notice at Collection Strategies

- **Identify Categories Collected and Purposes Used, and By Whom**
- **Single Notice versus Separate Notices**
- **Additional Content?**
- **Broad versus narrow notice**
- **California residents only?**
- **Service providers**

Private Cause of Action

- Nonencrypted and nonredacted **personal information** is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's **violation of the duty to implement and maintain reasonable security procedures and practices** appropriate to the nature of the information to protect the personal information
- **Personal information:**
 - First name or first initial, and last name in combination with:
 - Social security number;
 - Driver's license number or CA ID card number;
 - Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access;
 - Medical information; or
 - Health insurance information
- **Reasonable safeguards:**
 - Center for Internet Security (CIS) 20 controls

Private Cause of Action

- Up to **\$750/consumer per incident** (but not less than \$100) in statutory damages, based on:
 - *Nature and seriousness of misconduct*
 - *Number of violations*
 - *Persistence of the misconduct*
 - *Length of time misconduct occurred*
 - *Willfulness of misconduct*
 - *Defendant's assets, liabilities, and net worth*
- 30-day cure period – prior to individual/class action
- Written notice identifying specific provisions allegedly violated
- No notice if actual pecuniary damages suffered



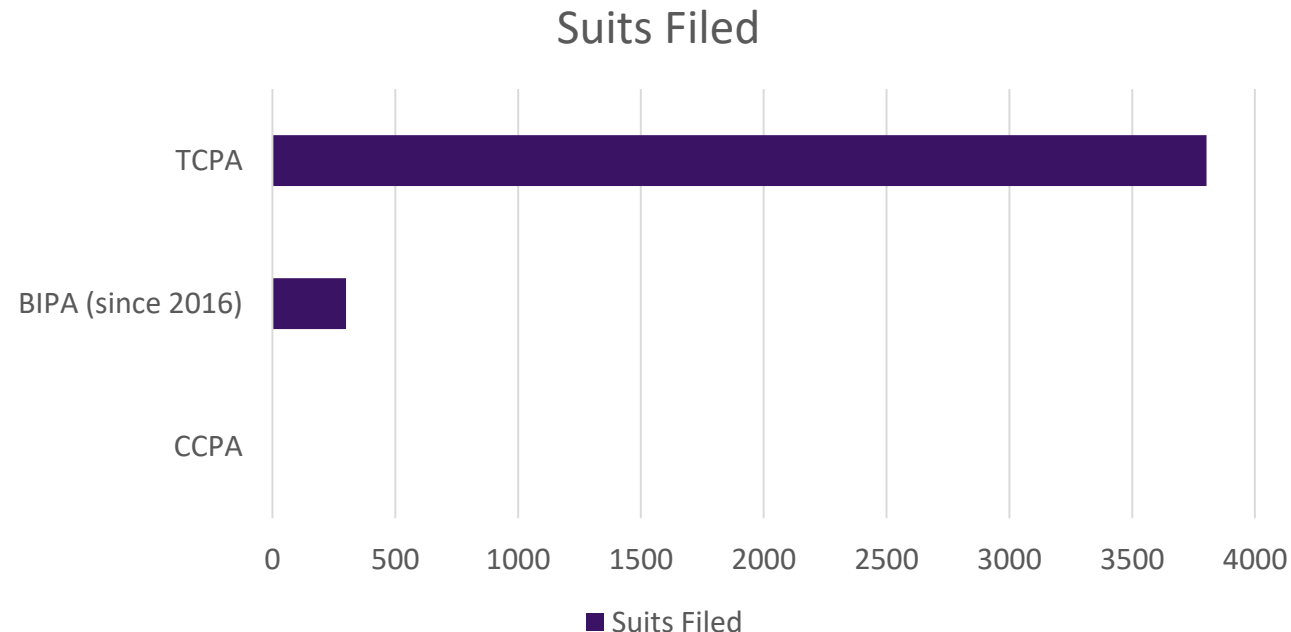
Why Statutory Damage Provision Matters

What has data breach class action litigation meant for plaintiffs?

- Circuit courts split regarding standing (Article III) post *Spokeo, Inc. v. Robins*
- Key question – whether plaintiffs must demonstrate an “injury-in-fact” has occurred that is both concrete and particularized
 - Does a “risk of future harm” qualify as such an injury
 - 3rd, 6th, 7th, 9th and D.C. circuits have generally found standing
 - 1st, 2nd, 4th and 8th circuits have generally found no standing

Why Statutory Damage Provision Matters

- **CCPA - real or concrete injury not required**
- Similar to (i) Telephone Consumer Protection Act (TCPA) (\$500 - \$1500), and (ii) Illinois' Biometric Information Privacy Act (BIPA) (\$1,000 - \$5,000)

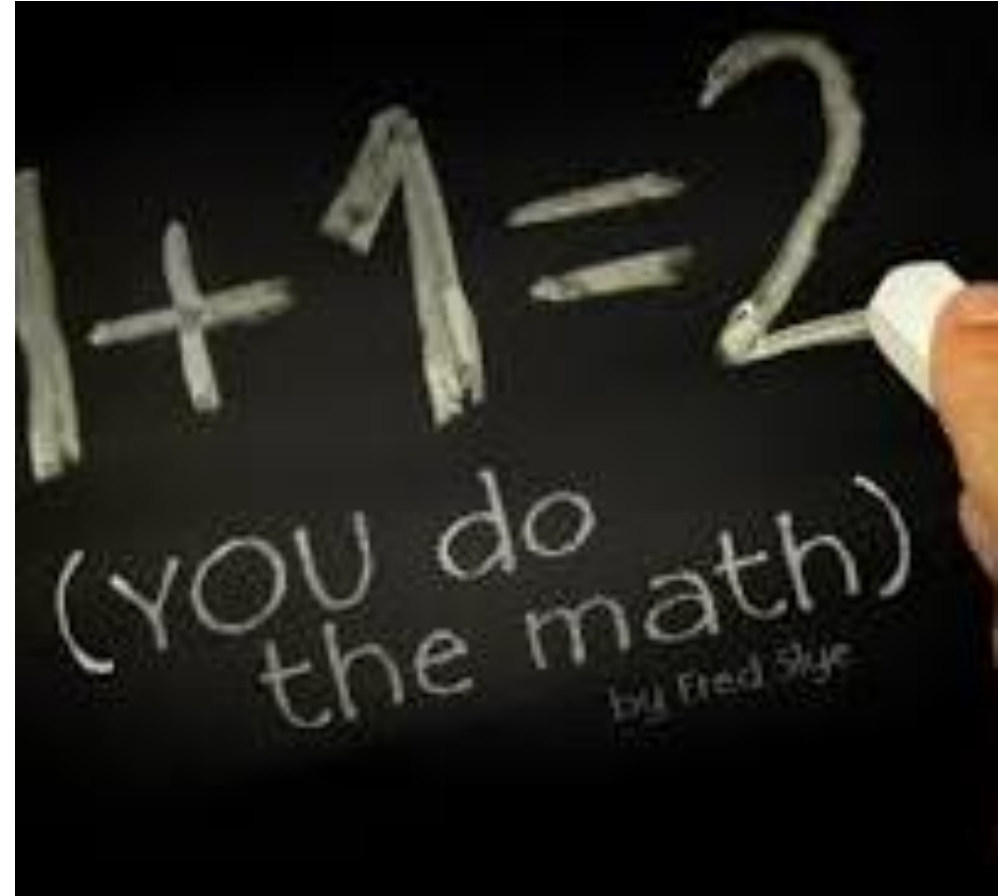


Why Statutory Damage Provision Matters

***3 in 5 Californians
were victims of a
data breach***

***40 million
Californians as of
2018***

***24 million potential
victims
(\$100-750/person)***



How to Prepare

- Inventory of PI collected, processed, and disclosed
- Review security infrastructure for reasonable safeguards
- Update and publish privacy policies and notices
- Coordinate with third party service providers
- Processes and procedures; identify key staff
 - Two mechanisms to make requests (email, post, web, phone, etc.)
 - Manage information, access, deletion, and opt-out requests
 - Train designated employees
- Watch for regulations/updates to law



JacksonLewis

Thank **you.**