Privacy at the Table:

Practical Strategies for California Consumer Privacy Act Compliance and Beyond

---

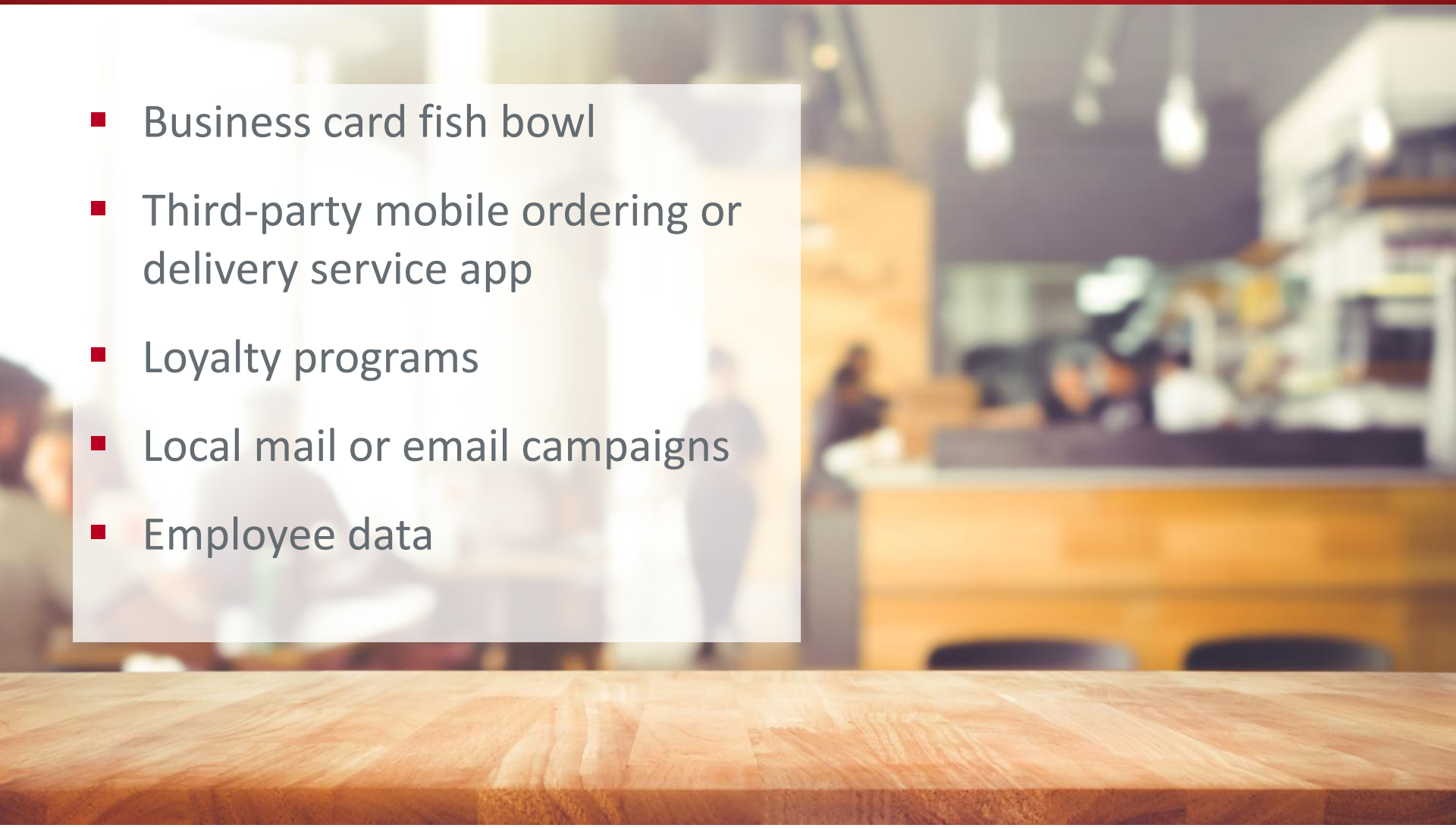
Presented by Helen Goff Foster & Aaron Colby

What's Cooking?

California Consumer Privacy Act (CCPA) is NOT just another state privacy statute

- Requires brand-wide compliance
- Broad definition of personal information
- Applies to online and offline information
- Private right of action for common breaches
- Provides consumer access and deletion rights upon request across business lines and points of collection
- Apparent persistent opt-out across devices and methods of interaction

What does this have to do with Restaurants?



- Business card fish bowl
- Third-party mobile ordering or delivery service app
- Loyalty programs
- Local mail or email campaigns
- Employee data

CCPA Overview: Covered Entities

Any commercial (for-profit) enterprise that:

Does business in the State of California (*including any same-branded controlled or controlling company*); and

Meets any one of the following:

- gross revenues of more than $25 million;
- receives or shares Personal Information (PI) for more than 50,000 "consumers, households, ***or*** devices"; or
- receives more than 50 percent of its annual revenue from the sale of PI

CCPA Overview: New Consumer Rights At A Glance

Consumer access to PI

Delete PI upon request

Respect Opt-out of sale of PI

CCPA Overview: Scope

- Personal Information: "information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly with a particular *consumer or household*."


IP address


Geolocation


Email address


Biometrics


Products/services purchased


Internet/browsing history


Education/FERPA info


Employment info


Inferences/profiles


Olfactory information

This isn't Grandma's Recipe for PI

- Privacy and security controls must be brought to apply on an expanded definition of "personal information"

GDPR/EPRIVACY

"[A]ny information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."

FTC Statements

"We regard data as "personally identifiable," and thus warranting privacy protections, when it can be reasonably linked to a particular person, computer, or device. In many cases, persistent identifiers such as device identifiers, MAC addresses, static IP addresses, or cookies meet this test."
Keeping up with the Online Advertising Industry, Jessica Rich, April 21, 2016

CCPA

"[I]nformation that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household," including:

- "Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier Internet Protocol address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers."
- "Commercial information, including records of personal property, products or services purchased, obtained, or considered . . ."
- Biometric information.
- "Professional or employment-related information."
- "Inferences drawn . . . to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, preferences, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes."

California Shine the Light, Cal. Civ. Code 1798.80 et seq.

"[A]ny information that when it was disclosed identified, described, or was able to be associated with an individual," including:

- An individual's name and address, telephone number, electronic mail address, age or date of birth,
- Names of children, electronic mail or other addresses of children, number of children, age or gender of children.
- Height, weight
- Race, religion, political party affiliation
- Occupation.
- Education.
- Medical condition.
- Drugs, therapies, or medical products or equipment used.
- The kind of product the customer purchased, leased, or rented.
- Real property purchased, leased, or rented.
- Social security number, bank account number, credit card number, debit card number.

PI Collection in Restaurants

Payment card data

3rd Party Payment Processor

Ma Foster Corporate/ Franchisor

wallet

Cell phone & payment card data

Mobile order app

Business card fishbowl (professional id info)

Ma Foster's Restaurant

Affiliated Brand Restaurant

IP address, cookies

website

Ma Foster's Restaurant #2

Spouse's email

Foster's loyalty club

CCPA Overview: New Consumer Rights

CCPA provides new consumer rights to control personal information.
Businesses must:

Provide consumer access to PI:

Twice annually, upon "verifiable consumer request," must provide consumers with "specific pieces" of PI collected about them in the previous 12 month period.

Delete consumer PI:

Honor consumer requests to delete PI from their systems and direct service providers to do the same, subject to several exceptions.

Respect consumer requests to opt-out of "sale" of PI:

Facilitate and implement persistent opt-out (across product/business line)

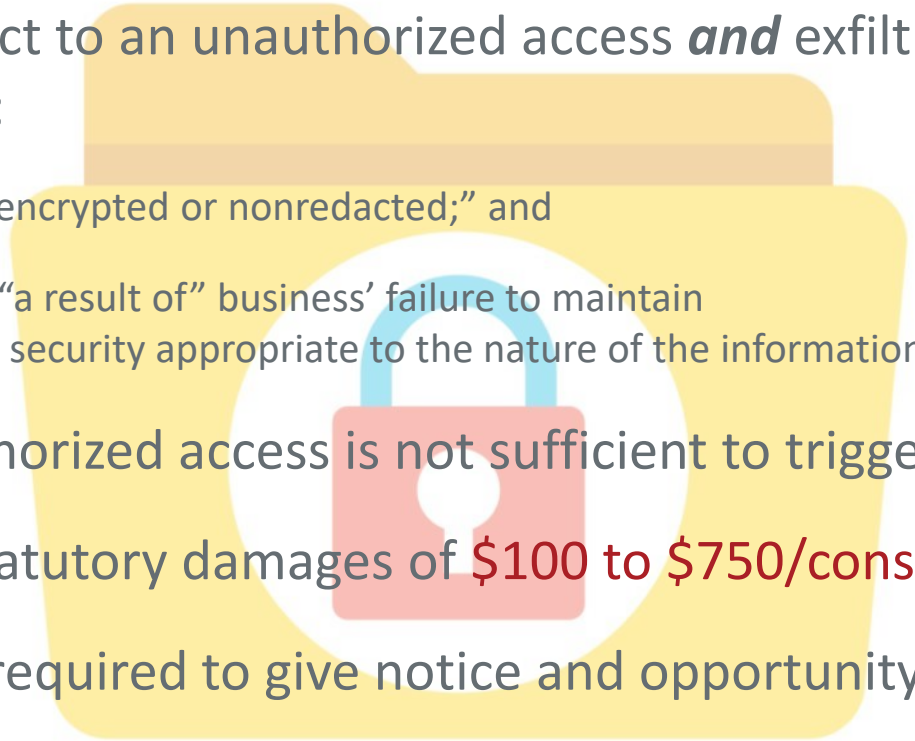
- Cannot request consumer to opt back in for 12 months

CCPA Overview: Enforcement

- **The Attorney General of California can bring suit against any business who violates any provision of the law**
  - **Businesses have 30 days to cure a violation**
- **Fine of up to $2,500 per violation, and $7,500 for intentional violation**
  - **Each impacted consumer constitutes one violation**

CCPA Overview: Data Security

- CCPA creates a private right of action for any consumer whose PI (limited in this instance to PI as defined in existing breach notification law) is subject to an unauthorized access ***and*** exfiltration, theft, or disclosure if:
  - PI was "nonencrypted or nonredacted;" and
  - Breach was "a result of" business' failure to maintain "reasonable security appropriate to the nature of the information."
- Mere unauthorized access is not sufficient to trigger liability
- Minimum statutory damages of $100 to $750/consumer/incident
- Consumers required to give notice and opportunity to cure



CCPA Compliance at a Glance

1. Assess current status and abilities
2. Data and systems mapping
3. Review information governance and security program, including service provider disclosures
4. Implement consumer response protocols
5. Update policies, procedures, and training

CCPA Soup to Nutz: Follow the Brand

CCPA's definition of "business" includes entities with a common brand and "management control"; appears to require an enterprise-wide (brand-wide) approach:

- **IMPACT: Franchisors could be held responsible for franchisee non-compliance, if common brand and maintain control over management**

  - » Nearly every provision of the CCPA requires businesses to be able to identity and retrieve all of the PI related to a specific consumer across business units and product/service lines.
  - » Does your business have accurate maps of how and where PI is stored enterprise wide? Can you efficiently index or relate all of the PI your business to identify, retrieve, and disclose that PI promptly to any individual consumer who may request it?

- **IMPACT: Ensure data use and disclosure restrictions implemented fully enterprise/brand-wide**

  - » CCPA requires businesses to provide details of their practices related to the collection, use, and disclosure of PI, and to update those notices at least once a year. More detailed disclosures that cover multiple business lines inevitably increases opportunities for inaccuracies.
  - » Inaccurate notices opens the door to potential enforcement actions under CCPA, the California Consumers Legal Remedy Act and Section 5 of the Federal Trade Commission Act

CCPA Soup to Nutz: Access Requests

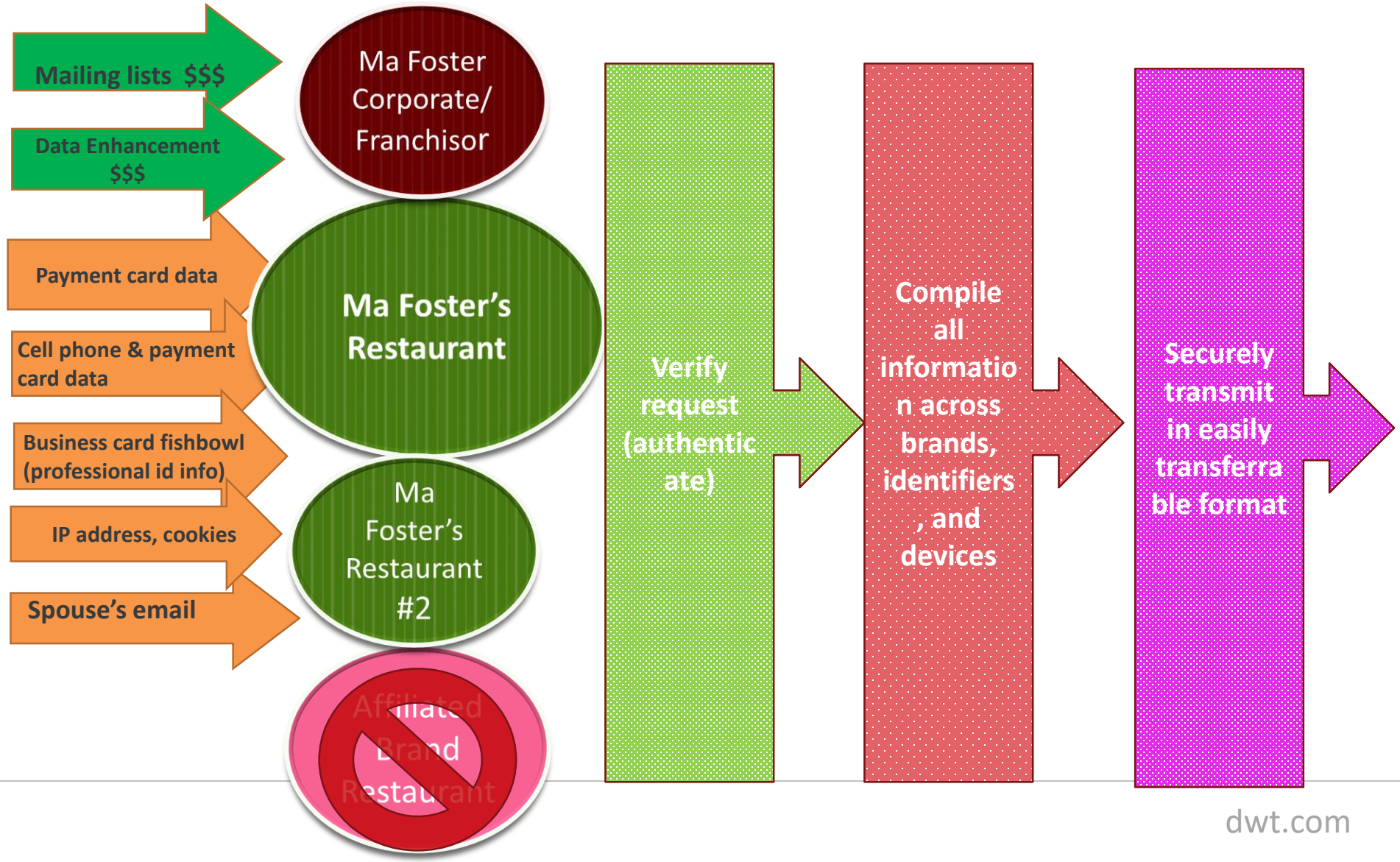
CCPA requires businesses to implement complex methods to facilitate consumer requests for access to PI and to fulfill such requests.

- **IMPACT: Businesses must implement at least two methods (including a toll-free number) to allow consumers to make a "verifiable" request**
  - Businesses must be able to verify the identity of the consumer making the request (or his/her authorized representative)
  - "Verifiable" requests subject to AG rulemaking; currently the statute prohibits businesses from requiring a consumer to create an account to make such a request

- **IMPACT: Businesses must implement a secure way to provide PI to consumers**

  - Once a request is verified, the business must disclose the **"specific pieces" of personal information** a business has collected regarding that individual, as well as the categories of PI collected, where it was collected from, the business purpose for the collection, and the categories of entities to whom personal information is sold or disclosed for a business purpose
  - If the information is provided in an electronic format, **it must be portable** and, to the extent technically feasible, in a readily useable format that allows the consumer to transmit this information to another entity without hindrance.
  - Such disclosures, if not carefully implemented, easily could become the **target of fraud/criminal actors** and thus the basis for claims of unauthorized disclosure of PI, resulting in liability under the CCPA.

Consumer Right of Access Under CCPA



CCPA Soup to Nutz: Right To Be Left Alone?

CCPA's right to perpetual opt-out and to be free from requests to opt back in

- **IMPACT: For a consumer who opts out, the business' interactions with that consumer over the 12 months following the opt-out cannot include a request to opt-back in.**
  - This represents a major implementation challenge for heavily matrixed organizations, such as the prohibition on requesting permission to sell the consumers data applies to all types of PI and must be honored enterprise-wide, across business lines, and across methods of consumer interaction (including across devices, browsers, etc.
  - This provision could be read as an invitation to track consumer interactions more closely in order to promote compliance.
  - Potential conflict with consumer's right to delete data, but retention for tracking compliance likely falls within one of the exceptions

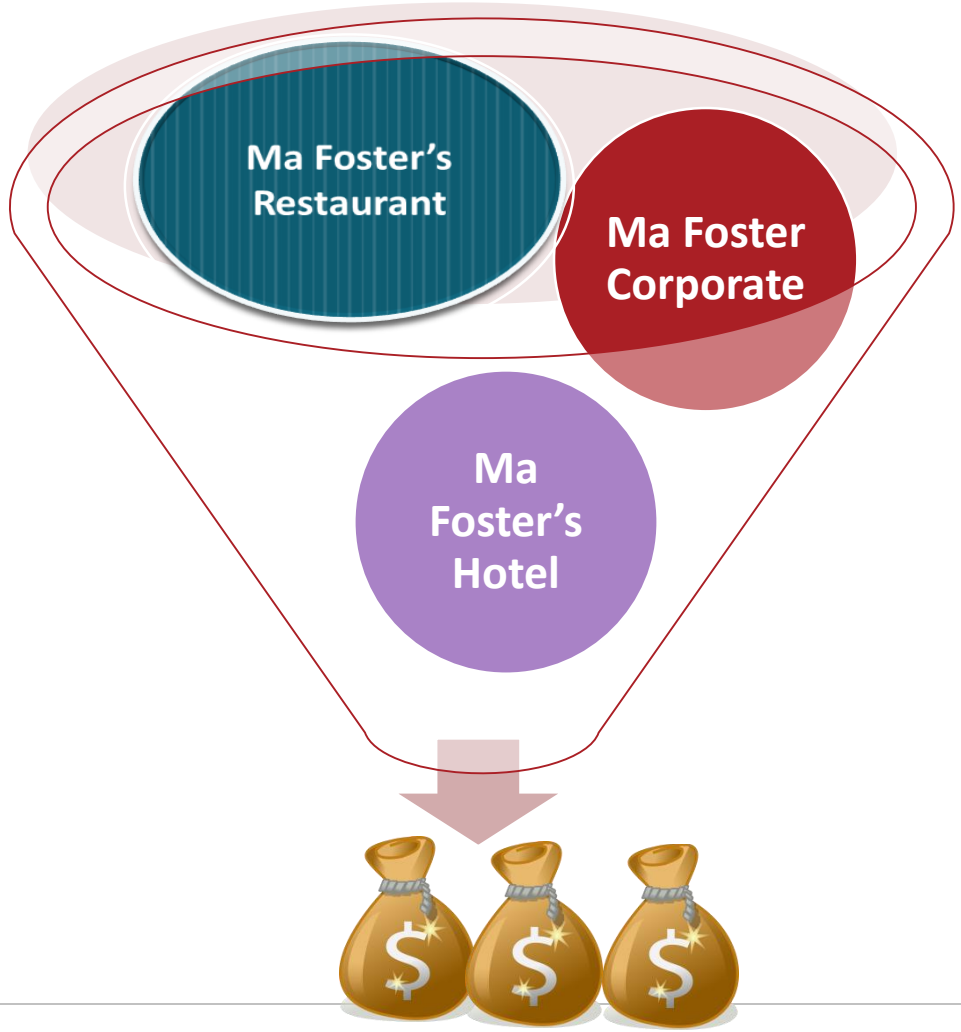
CCPA Soup to Nutz: External Party Relationships

- External parties with whom data is shared are either **“third parties” or “service providers.”**
- **Service Providers:** Consumer cannot opt-out of sharing information with vendor/service provider

- **IMPACT:** Service provider agreements will need to be amended to require service providers to restrict use of data to purpose of contract
- **IMPACT:** Businesses not otherwise subject to the CCPA may encounter issues where they provide services to businesses who are

Private Right of Action under CCPA

=



CCPA Soup to Nutz: Unfounded Lawsuits

CCPA effectively supplements the California Data Breach Notification Law with a private right of action, for unauthorized access/disclosure of both electronic and non-electronic PI.

- **IMPACT: Businesses must affirmatively demonstrate implementation of reasonable security measures to defend such suits**
  - Consumers do not have to demonstrate harm or actual losses to recover under CCPA.
  - "Reasonable security" is not defined under California law, the Attorney General ("AG") has previously cited the 20 controls in the Center for Internet Security's Critical Security Controls as identifying a minimum level of information security that all organizations that collect or maintain personal information should meet.
  - Credible third party security and compliance assessments could be key to defending against CCPA suits
  - Potential attempt to limit arbitration agreements

CCPA Soup to Nutz: Required Notices

CCPA increases requirements for detailed and conspicuous notices and opt-out

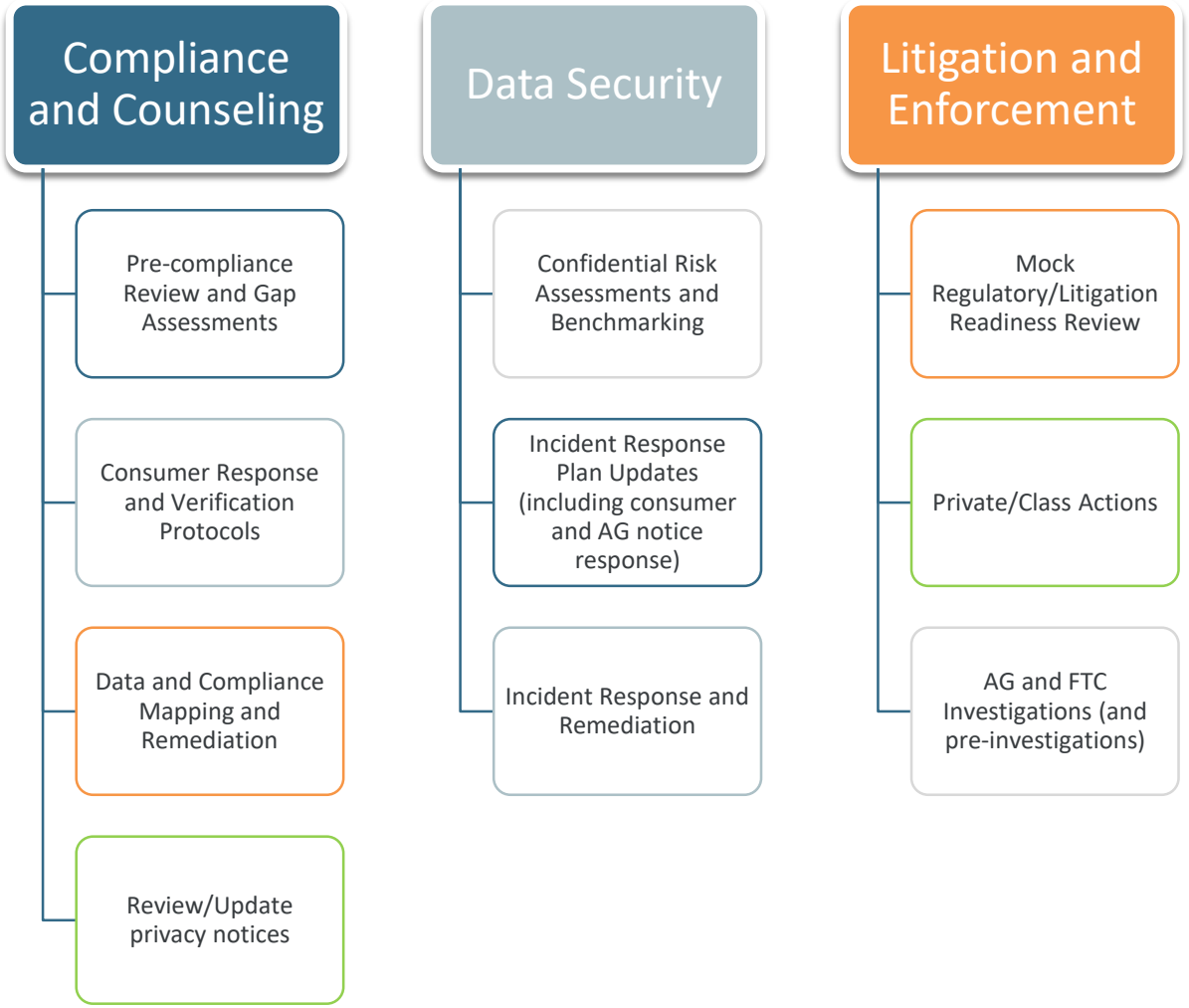
- **IMPACT:** Businesses that engage in the "sale" of PI must inform consumers specifically that their information may be sold to third parties and that they have the right to opt-out in both online and offline privacy policies.

- Requires use of website link on the business' homepage titled "*Do Not Sell My Personal Information.*"
- CCPA allows for creation of separate California-only home pages that contain these links.
- Businesses must also notify consumers of any financial incentives they offer to influence the consumer's choice on this webpage.
- All customer service personnel must be trained on the new consumer rights afforded by the CCPA and how a consumer may exercise them

CAUTION:

- Effective date is January 2020:
  - AG cannot enforce until July 2020

DWT Helps Our Clients Stay Out of the Soup!



DWT Disclaimer

This presentation is a publication of Davis Wright Tremaine LLP. Our purpose in making this presentation is to provide Citi Cards with general information, not specific legal advice (as such advice counsel may be given only in response to inquiries regarding particular situations).

Davis Wright Tremaine LLP
DEFINING SUCCESS TOGETHER