# 2020
# Barrett McNagny Virtual Seminar
## Wednesday, September 2, 2020

# Cybersecurity & Data Privacy:
## Workplace Data in the Information Age

By: James J. O'Connor
215 E. Berry Street
Fort Wayne, IN 46802
Direct: (260) 423-8868
jjo@barrettlaw.com

Barrett McNagny LLP
ATTORNEYS AT LAW

# James J. O'Connor

## Partner

**Phone: 260-423-8868**
**Fax: 260-423-8920**
**Email: jjo@barrettlaw.com**

James O'Connor has experience in representing businesses, insurers, and individuals through the legal system in matters involving jury trials, employment disputes, cybersecurity, contract disputes, insurance litigation, insurance coverage analysis, workers compensation, employment litigation, HR investigations, and data breach response.

James is ranked an AV® Preeminent™ rated attorney based on Martindale-Hubbell's peer review ratings and was selected for inclusion in the 2021 *Best Lawyers® in America* publication for labor law- management. He is or has been a member of associations such as the Allen County Judicial Nominating Commission, the Benjamin Harrison chapter of the American Inns of Court, and the Defense Research Institute. He was selected for inclusion in the 2018 Indiana *Super Lawyers®* publication in the field of litigation. James regularly presents at local and statewide seminars on employment topics, including cybersecurity protection, data breach response, and worker's compensation matters.



1876

# Glossary

- Cybersecurity
  - "Measures taken to protect a computer or computer system (as on the internet) against unauthorized access or attack."
    - Merriam-Webster Online: https://www.merriam-webster.com/dictionary/cybersecurity
- Data Breach
  - "the loss, theft, or unauthorized access, other than those incidental to the scope of employment, to data containing sensitive personal information, in electronic or printed form, that results in the potential compromise of the confidentiality of integrity of the data." 38 USCA §5727(4)
  - "unauthorized acquisition of computerized data that has been transferred to another medium, including, paper, microfilm, or a similar media, even if the transferred data are no longer in a computerized format." IC §24-4.9, et seq.
- Personal Information
  - "SSN or person's name in combination with one or more of the following elements: driver's license number, account number, a state ID card number, a credit card number, a financial account number in combination with any required security code." IC §24-4.9, et seq
  - "Any 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." CCPA
- Data Privacy
  - Policies regarding the use and governance of personal data and how it is collected or shared. International Association of Privacy Professionals (IAPP); https://iapp.org/about/what-is-privacy/

# What's the Difference?

- **Security**
  - Protection from Unauthorized Access
  - Think: encryption; preventing a breach / hack; protection from bad actors

- **Privacy**
  - Policies to govern use of Personal Information (PI)
  - Think: how businesses can use Consumer details; medical records; financial data; website data

# Cybersecurity – Bad Actors' Tools of the Data Breach Trade

- **Malware** – program that infects a computer/device and carries a malicious code to destroy data on the machine or permit another to control your computer/device
  - **Virus** – usually an executable file that does no damage until malicious program is opened or run; often shared via attachment to an email
  - **Worm** – can replicate itself on system; travel between computers without assistance
  - **Trojan horse** – appears as useful software but will do damage once installed or run; often creates a back door that unauthorized users will later exploit; do not self replicate and do not reproduce by affecting other files.
- **Phishing/Spearphishing** – using fake website or email to lure victim into providing personal information or fraudulent instructions for financial transaction.
- **Spyware** – software that sends information from your computer to a third party without your consent
- **Social Engineering** – technique used by cybercriminals designed to lure unsuspecting users into sending them confidential data or infecting their computers with malware.
- **Vishing /Smishing** – spam VoIP calls or voicemails (or SMS texting) purportedly from reputable companies attempting to get recipient of phone call to disclose personal information such as bank or credit card details.

# COVID-19 & "Shelter In Place"

- Since March 2020 – significant increase in telework, shopping online and digital connections to the world at large.
- FBI's Cyber Division estimates close to 4,000 Cyber Attack complaints per day
  - As of August 11, 2020
  - 400% increase from pre-Covid activities
  - Cyberattacks of governments, major corporations including healthcare providers
- Use of Phishing or social engineering attacks up 20k – 30k per day in the United States alone.
- Ransomware attacks up 800% since pandemic.
  - https://www.prnewswire.com/news-releases/top-cyber-security-experts-report-4-000-cyber-attacks-a-day-since-covid-19-pandemic-301110157.html
- July 15 Twitter hack. A 17 year old in Florida orchestrated the hack of the 'Verified' twitter accounts of many celebrities and policitians. Scam netted about $117,000.
  - Was accomplished with combination of traditional hacking and social engineering. The hacker convinced a Twitter employee (likely working from home) that he was a fellow Twitter employee and using a SIM-swap with a telephone carrier.

1876

# Goals for Cyber Breach Response

- **Establish clear communication**
  - Internally (inform employees and vendors retained to respond)
  - Externally (victims whose information has been breached)
  - Establish a Response Team
- **Determine what happened**
  - Forensic analysis to evaluate how loss occurred
  - Take immediate steps to remedy the problem
- **Determine the scope of exposure or harm**
  - Database encrypted?
  - What kind of information was exposed: SSNs, DOBs, addresses, credit card information
- **Change Passwords**
- **Trigger event for Cybersecurity Insurance**
- **Research notice laws of applicable states where you work / Contact your legal counsel**
  - Victims receive notice
  - Government agencies receive notice
- **Research state laws to determine Scope of Breach Fallout**
  - Statutory damages to victims
  - Credit monitoring benefits

# Cybersecurity –Indiana Data Breach Notification Statutes IC §24-4.9-et seq.

- Trigger to potential victims: if the database owner knows, should know, or should have known that the unauthorized acquisition constituting the breach has resulted in or could result in identity deception, identity theft, or fraud affecting the Indiana resident
- Notice must be made "without unreasonable delay" by mail, telephone, fax or email.
- Notice to the "Big 3" Consumer Credit Reporting Agencies if more than 1,000 Indiana residents are effected
- This is a "Risk of Harm" analysis emphasis on potential impact on Hoosier victim
- Also applies if PII is not still in digital form – if printed off and still acquired
- Trigger to Notify Attorney General
  - Failure to make required disclosure constitutes a deceptive act
  - Subject to injunction, civil penalties, and Attorney General's reasonable costs
- Encryption makes Database owner exempt from compliance
  - So long as bad actor did not get encryption key

1876

# Other Data Breach Notification statutes

- Notice to potential victims triggered by “unauthorized access” into holder of information
  - emphasis on duty to protect information
- Notice required within a specific time frame
  - Other than general provision that notice by given in the most expedient time and manner possible and without unreasonable delay, consistent with the legitimate needs of law enforcement
  - Example: Ohio: Most expedient time possible but not later than 45 days following discovery of the breach
  - Days as little as 30 (FL) to 90 (Conn)
- 17 states/territories permit Private Cause of Action
  - Not Indiana
  - Victims May seek Actual damages (LA & DC); Treble Damages (Mass); Equitable relief and atty fees (NH); not less than $1000 plus atty fees (NC); Not more than $5000 (NC)
  - Data Collector may sue violator (Nevada)

# Federal and State Agencies – Post Attack

- File a report with the Office of the Inspector General (OIG) if you think someone is illegally using your Social Security number.
- File a complaint with the FBI Internet Crime Complaint Center (IC3). They will review the complaint and refer it to the appropriate agency.
- File a report with the local police so there is an official record of the incident.
- Report identity theft to the Federal Trade Commission.
  - FTC has been tracking specific complaints since January 1, 2020
  - In Indiana: 1,802 complaints filed related to Fraud, ID theft, credit card or financial crimes
  - In total, approximately $904k or average about $501.66 per complaint.
  - In USA: 176k complaints; $118.15M lost
- Contact additional agencies depending on what information was stolen. Examples include contacting the Social Security Administration (800-269- 0271) if your social security number was compromised, or the Department of Motor Vehicles if your driver's license or car registration has been stolen.
- Report online crime or fraud to your local United States Secret Service (USSS) Electronic Crimes Task Force or the Internet Crime Complaint Center.

# Takeaways: Protection Measures

- Password policies – complexity/mandatory changes for time or event
- Firewall/anti-virus software protection
- Encryption
- Handbook Policy and Software for enforcement of restrictions on internet access
- Keep operating system updated

# Data Privacy: General Data Protection Regulation (GDPR)

- What is the GDPR?
  - Rules instituted by the European Union related to handling Consumer Data concerning EU residents
- When did it go into effect?
  - May 25, 2018
- Who benefits and who is subject to regulation?
  - Individuals (called ‘data subjects’), Organizations and Companies who are ‘Controllers’ or ‘Processors’ of EU residents’ personal data in the context of an EU establishments’ activities, regardless whether the data processing takes place in EU.
  - **Non-EU data controllers with no EU establishment that offer goods or services to individuals in the UE or monitor their behavior that takes place in the EU.**
- What is Personal Data under GDRP?
  - Name, address, IP address, DOB, genetic information, political views, sexual orientation

# GDPR cont'd

- Protections EU residents receive:
  - Easier access to the data companies have on individual, such as:
  - 'Monitoring' – organizations tracking individuals on the internet and use personal data to:
    - profile a natural person to make decisions concerning him or her; analyze or predict personal preferences, behaviors and attitudes.
    - Geolocation tracking for marketing purposes; data collection through wearables
    - Closed circuit television camera use
  - 'profiling' – any form of automated processing of personal data about a person to analyze or predict:
    - Performance at work; economic situation; health; personal preferences or interests; location or movements
- Enforcement mechanism:
  - Monetary Fines
    - Small offenses: greater of €10 million or 2% of a firm's annual revenue
    - Serious offenses: greater of €20 million or 4% of a firm's annual revenue
  - Criminal Penalties
    - Which may allow for the 'deprivation of profits' obtained through GDPR infringments
  - Data Subject lawsuits
    - Filed directly against 'data controllers' or 'data processors'
    - Lodge a complaint; seek compensation for material/immaterial damage

# So what, that's the European Union…

- January 1, 2020 - California's Consumer Protection Act (CCPA) went into effect for compliance purposes
- July 1, 2020 – California's Attorney General begins enforcement
- Who benefits?
  - "Consumers" - California residents / natural persons:
    - In CA 'for other than a temporary or transitory purpose;' or
    - Domiciled in CA but currently outside CA for a temporary or transitory purpose.
    - Likely includes CA-based Employees and/or contacts from business customers or vendors
- What is protected?
  - Personal Information ("PI"): Any 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."
- PI does NOT include:
  - information lawfully made available from government records;
  - deidentified or aggregate consumer information
    - Note: Compare against Indiana's definition; we're beyond SSNs in combination with DOBs and addresses

# CCPA's 11 Personal Information Categories

1) **Identifiers**: Real name(s); an alias; postal address; email address; unique personal or online identifier; an Internet Protocol (IP) address; an account name; Social Security Number (SSN); Driver's License or Passport Number; another form of persistent or probabilistic identifier that can identify a particular consumer, family, or device.

2) **PI as defined in CA's "Customer Records" statute**: Signature; State ID card; Physical characteristics or description; Insurance policy number; Education; Employment or employment history; Bank account number, credit card number, debit card number or any other financial information; or Medical information or health insurance information.

# CCPA's 11 Personal Information Categories (con't)

3) **Protected Class Characteristics** under federal or CA law: race, national origin, religion, gender, sexual orientation

4) **Commercial information**, including personal property records or purchasing habit records

5) **Biometric Information**:
   - Genetic / physiological / behavioral / biological characteristics from which organizations can extract a template or other identifying information
   - Examples:
     - fingerprints / faceprints / voiceprints
     - iris or retina scans
     - keystroke, gait or other physical patterns; and
     - sleep, health, or exercise data

6) **Internet or other similar network activity**, such as:
   - Browsing history;
   - Search history;
   - Information regarding a consumer's interaction with an internet website, application or advertisement

# CCPA's 11 Personal Information Categories (con't)

7) **Geolocation data**

8) **Audio, electric, visual, thermal, olfactory** or similar information

9) **Professional or employment-related information**

10) **Non-publicly available educational information** as defined under the Family Educational Rights and Privacy Act (FERPA)

11) **Inferences** drawn from other PI to create consumer profiles reflecting:

- Preferences;
- Characteristics;
- Psychological trends;
- Predispositions;
- Behavior;
- Attitudes;
- Intelligence;
- Abilities; or Aptitudes

Note: manner of data collection is irrelevant. CCPA applies to PI collected or generated electronically on a computer; online over the internet; using a pen and paper; through an algorithm.

# CCPA applies to what Businesses?

"Business" is a 'for-profit entity, including sole proprietorship, partnership, LLC, Corp., Association or other legal entity' that:

- Collects a Consumer's PI (directly or through an agent) and determines the purposes and means of processing.
- Does business in CA and meets one of the following criteria:
  - Annual gross revenue exceeding $25M (adjusted for inflation);
  - Annually buys, receives, shares or sells the personal information of more than 50k consumers / households / devices for commercial purposes (alone or in combination)
  - Derives 50% or more annual revenue from selling consumer's personal information

# CCPA Regulations

- Entities conducting business in CA have duties related to data protection.
  - Applicable to business inside and outside the state of CA.
- CCPA regulations related to processing CA residents' PI include:
  - Creating or updating **privacy notices**;
  - Consumer choice requirements for selling personal information;
  - Restrictions on data monetization business models;
  - Accommodating consumers' rights to access their personal information;
  - Honoring the **right to deletion**;
  - Producing requested data in portable format.

# Limited Exceptions to PI definition and scope

**Commercial Conduct Wholly Outside of CA**

- Extraterritorial Exception: PI is collected while Consumer is outside CA; No part of sale of Consumer's PI occurs in CA; Sale may not include PI collected while Consumer was in CA
- This Exception expressly prohibits a business from avoiding CCPA's intent by storing Consumer's PI while present in CA (including on device) and then collecting Consumer's stored PI when the Consumer or the stored PI is later outside CA.

**Government records**

- PI does not include 'publicly available' information, but information must be lawfully available from federal, state or local government records.

**De-identified or Aggregated Data**

- **De-identified Data**: cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked directly or indirectly, to a particular Consumer, if the business using the de-identified information:
  - Implemented technical safeguards that prohibit re-identifying the consumer to whom the information may pertain;
  - Implemented business processes that specifically prohibit re-identifying the information;
  - Implemented business processes to prevent inadvertent release of de-identified information; and
  - Makes no attempt to re-identify the information.
- **Aggregated Data:** information related to a group or category of consumers:
  - From which individual consumer identities were removed; and
  - That is not linked or reasonably linked to any consumer or household, including via device.

# PI Sale vs. PI Disclosure For Business Purpose

- To comply with CCPA, businesses must classify each transfer of PI to another entity as either: a sale or a disclosure for a business purpose.
- a PI sale creates more obligations on businesses than a PI disclosure for business purposes.
- In response to "verified consumer requests," businesses must provide two separate lists: one identifying sales and another identifying disclosures made for a business purpose.
- PI Sale includes any communication or transfer of a consumer's PI by a CCPA covered business to another business or third party for consideration (not just money).
  - A 'sale' includes acts of renting, releasing, disclosing, disseminating, making available, transferring or otherwise communicating PI in the following ways: orally, in writing, or electronically.
  - A 'sale' does not include PI transferred as an asset through a merger, acquisition, bankruptcy, or other transaction in which a third party assumes control of the business.

# PI Disclosure For Business Purpose

- A business may disclose PI for a 'business purpose use,' if the 'use' is for:
  1) an operational purpose of the business or service provider; or
  2) other notified purposes.

  The 'use' must be 'reasonably necessary for and proportionate to the operational purpose for which the PI is first collected or processed or another contextually compatible operational purpose.

- Seven (7) types of approved business purposes:
  1) Auditing the interaction with the consumer and concurrent transaction, including counting ad impressions and verifying quality of ad impressions;
  2) Detecting or preventing security incidents or other illegal activity and prosecuting the responsible parties;
  3) Debugging;
  4) short-term, transient use if the PI is not: disclosed to another third party and used to build a profile or otherwise alter an individual consumer's experience outside the current interaction;
  5) performing services on behalf of a CCPA-covered business or its service provider, such as customer service, order fulfillment, payment processing, financing and advertising, marketing or analytic services;
  6) undertaking internal research for technological development and demonstration; and,
  7) verifying or maintaining quality or safety or improving or upgrading a service or device owned, manufactured, or controlled by or for the business.

# CCPA's Consumer Rights

- General Notice rights
- Specific Information rights
- Data Portability Rights
- Deletion Rights
- Personal Information Sale Prevention Rights
- Freedom from Discrimination
- Prohibition on Waiver of Rights

# CCPA Consumers' General Notice Rights

Under the CCPA, Consumers have the right to know what PI a business collects, sells, or discloses about them, including the categories of third parties who purchased or received their data.

The CCPA spreads these obligations and rights out over several different sections of the statutes, including: consumer's right to know at a general level; consumer' rights when a business collects PI; consumer's rights when a business sells PI or discloses it for a business purpose.

These sections require both general notices about the business's overall activities and individualized notices providing detailed information about the person making a verified consumer request.

Under the "general information requirement," a business must disclose, before or at the point of collection, both: what PI categories the business collects, and the intended use purpose.

A business cannot collect additional PI categories or use collected PI for unrelated purposes without providing the required notice.

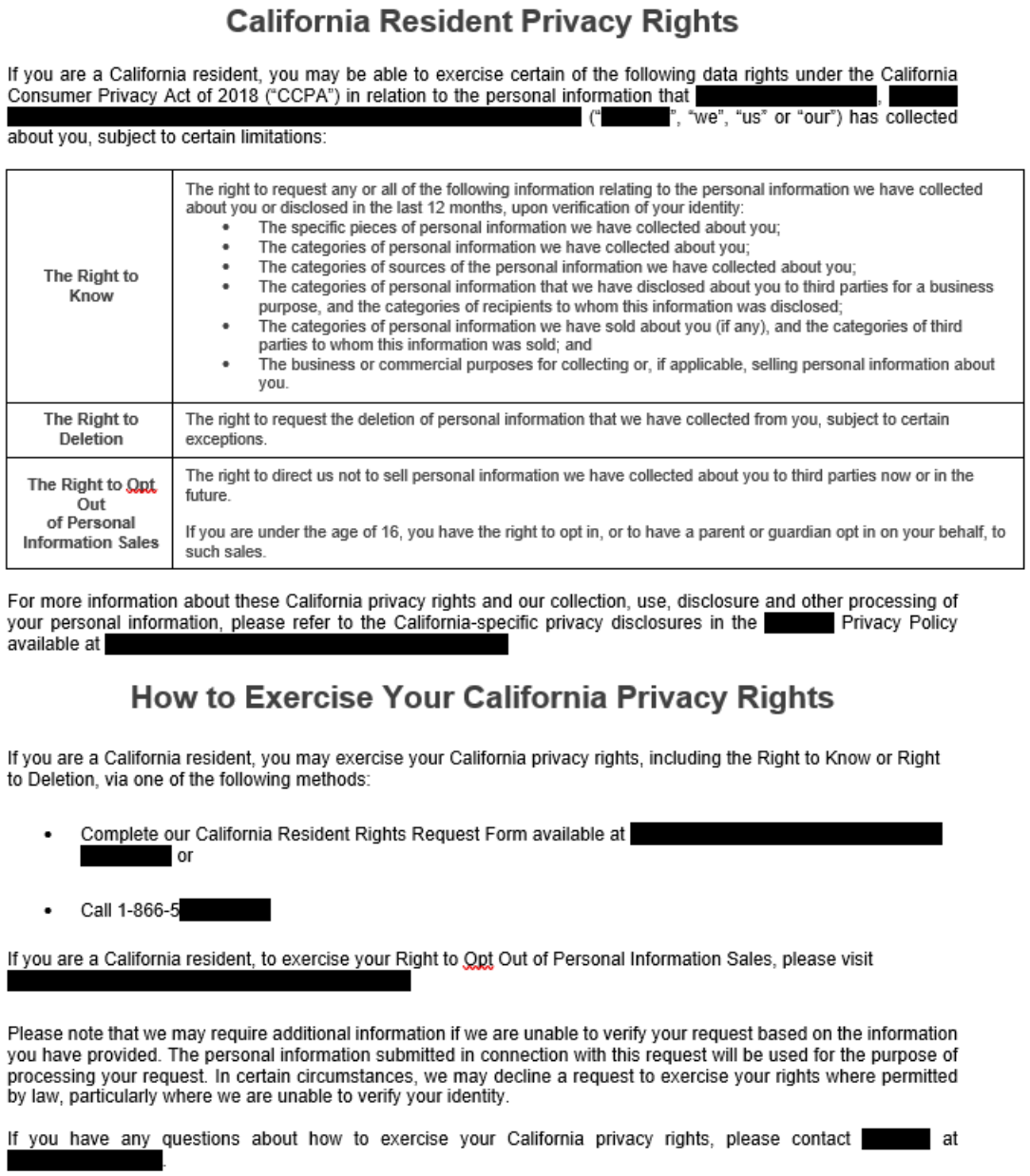
The CCPA operationalizes this general right to know by requiring the business to provide certain disclosures through privacy notices or other similar public statements.

# Notices at Collection

- A Notice at Collection must provide:
  - a list of the PI categories collected;
  - the business or commercial purpose for using each personal information category, separately;
  - a link or website address to the business' Do Not Sell My Personal Information notice, if applicable;
  - a link or website address to the business's privacy notice.

# Sample of General Notice

- Statement regarding CA residency requirement;
- Statement explaining the right to request any or all PI the business has collected or disclosed about you in the last 12 months;
- Statement explaining the right to request deletion;
- Statement explaining right to direct to not sell PI collected;
- Statement explaining how to exercise these privacy rights
- A link for Consumer to follow to complete a 'CA Rights Request Form" or a telephone number;
- A link on how to exercise the Right to Opt Out of PI Sales.



## California Resident Privacy Rights

If you are a California resident, you may be able to exercise certain of the following data rights under the California Consumer Privacy Act of 2018 ("CCPA") in relation to the personal information that [redacted] ("[redacted]", "we", "us" or "our") has collected about you, subject to certain limitations:

| | |
|---|---|
| The Right to Know | The right to request any or all of the following information relating to the personal information we have collected about you or disclosed in the last 12 months, upon verification of your identity:<br>• The specific pieces of personal information we have collected about you;<br>• The categories of personal information we have collected about you;<br>• The categories of sources of the personal information we have collected about you;<br>• The categories of personal information that we have disclosed about you to third parties for a business purpose, and the categories of recipients to whom this information was disclosed;<br>• The categories of personal information we have sold about you (if any), and the categories of third parties to whom this information was sold; and<br>• The business or commercial purposes for collecting or, if applicable, selling personal information about you. |
| The Right to Deletion | The right to request the deletion of personal information that we have collected from you, subject to certain exceptions. |
| The Right to Opt Out of Personal Information Sales | The right to direct us not to sell personal information we have collected about you to third parties now or in the future.<br><br>If you are under the age of 16, you have the right to opt in, or to have a parent or guardian opt in on your behalf, to such sales. |

For more information about these California privacy rights and our collection, use, disclosure and other processing of your personal information, please refer to the California-specific privacy disclosures in the [redacted] Privacy Policy available at [redacted]

## How to Exercise Your California Privacy Rights

If you are a California resident, you may exercise your California privacy rights, including the Right to Know or Right to Deletion, via one of the following methods:

- Complete our California Resident Rights Request Form available at [redacted] or
- Call 1-866-5[redacted]

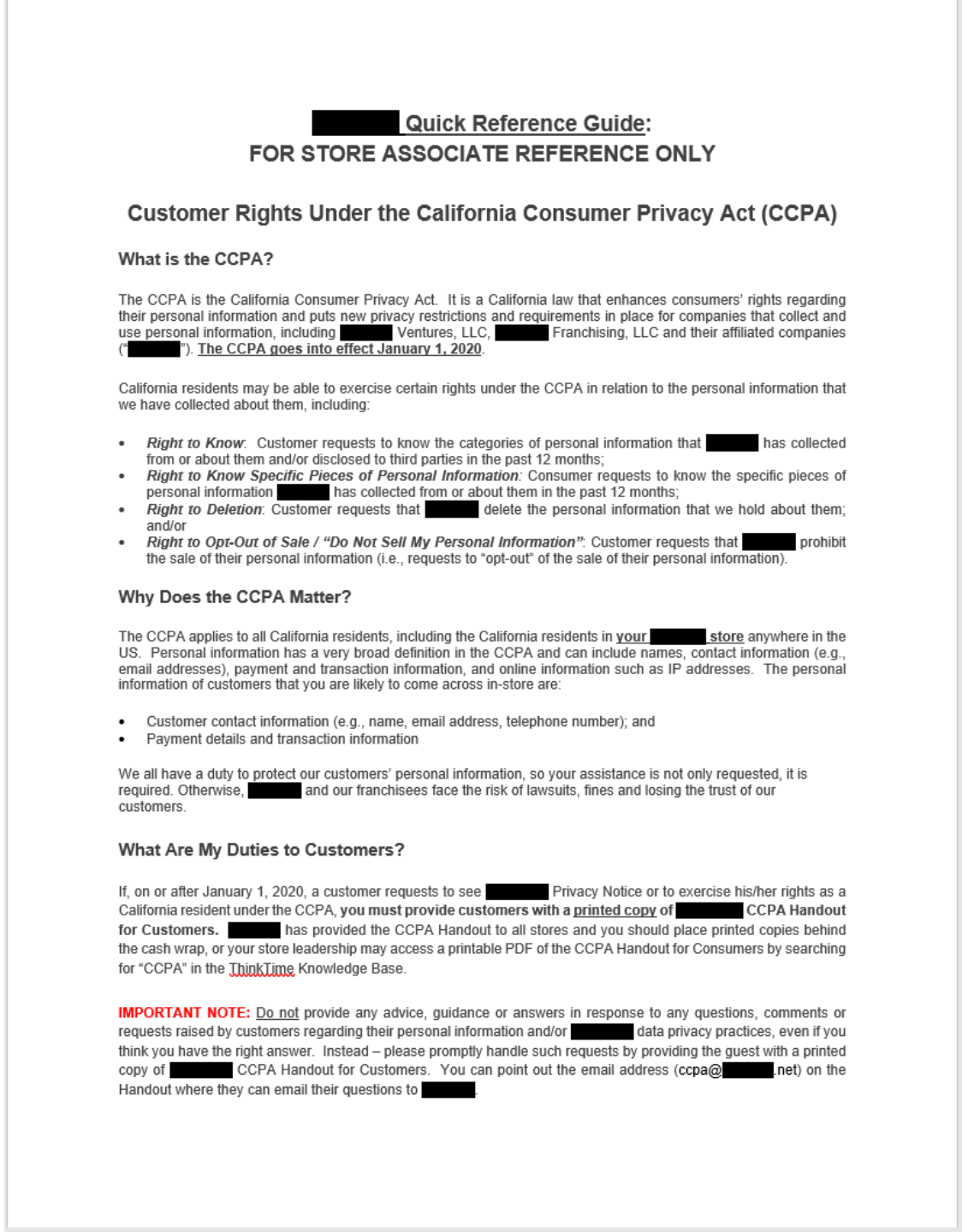
If you are a California resident, to exercise your Right to Opt Out of Personal Information Sales, please visit [redacted]

Please note that we may require additional information if we are unable to verify your request based on the information you have provided. The personal information submitted in connection with this request will be used for the purpose of processing your request. In certain circumstances, we may decline a request to exercise your rights where permitted by law, particularly where we are unable to verify your identity.

If you have any questions about how to exercise your California privacy rights, please contact [redacted] at [redacted].

# Sample for Employee Training

- Explains what the CCPA is
- Generally describes Consumer Rights
- Gives the Employee the general category of PI that will be collected at this kind of store
- Explains how to deal with Customers



[redacted] Quick Reference Guide:
FOR STORE ASSOCIATE REFERENCE ONLY

## Customer Rights Under the California Consumer Privacy Act (CCPA)

### What is the CCPA?

The CCPA is the California Consumer Privacy Act. It is a California law that enhances consumers' rights regarding their personal information and puts new privacy restrictions and requirements in place for companies that collect and use personal information, including [redacted] Ventures, LLC, [redacted] Franchising, LLC and their affiliated companies ("[redacted]"). The CCPA goes into effect January 1, 2020.

California residents may be able to exercise certain rights under the CCPA in relation to the personal information that we have collected about them, including:

- ***Right to Know***: Customer requests to know the categories of personal information that [redacted] has collected from or about them and/or disclosed to third parties in the past 12 months;
- ***Right to Know Specific Pieces of Personal Information***: Consumer requests to know the specific pieces of personal information [redacted] has collected from or about them in the past 12 months;
- ***Right to Deletion***: Customer requests that [redacted] delete the personal information that we hold about them; and/or
- ***Right to Opt-Out of Sale / "Do Not Sell My Personal Information"***: Customer requests that [redacted] prohibit the sale of their personal information (i.e., requests to "opt-out" of the sale of their personal information).

### Why Does the CCPA Matter?

The CCPA applies to all California residents, including the California residents in your [redacted] store anywhere in the US. Personal information has a very broad definition in the CCPA and can include names, contact information (e.g., email addresses), payment and transaction information, and online information such as IP addresses. The personal information of customers that you are likely to come across in-store are:

- Customer contact information (e.g., name, email address, telephone number); and
- Payment details and transaction information

We all have a duty to protect our customers' personal information, so your assistance is not only requested, it is required. Otherwise, [redacted] and our franchisees face the risk of lawsuits, fines and losing the trust of our customers.

### What Are My Duties to Customers?

If, on or after January 1, 2020, a customer requests to see [redacted] Privacy Notice or to exercise his/her rights as a California resident under the CCPA, **you must provide customers with a printed copy of [redacted] CCPA Handout for Customers.** [redacted] has provided the CCPA Handout to all stores and you should place printed copies behind the cash wrap, or your store leadership may access a printable PDF of the CCPA Handout for Consumers by searching for "CCPA" in the ThinkTime Knowledge Base.

**IMPORTANT NOTE:** Do not provide any advice, guidance or answers in response to any questions, comments or requests raised by customers regarding their personal information and/or [redacted] data privacy practices, even if you think you have the right answer. Instead – please promptly handle such requests by providing the guest with a printed copy of [redacted] CCPA Handout for Customers. You can point out the email address (ccpa@[redacted].net) on the Handout where they can email their questions to [redacted].

# Specific Information Rights

- The CCPA grants consumers an individualized "right to know" what PI a business collected, sold, or disclosed about them. These Information Access Rights also give consumers the right to obtain a copy of PI collected about them (see "Data Portability"). However, the CCPA tempers these rights by:
  - Requiring the consumer to verify their identity reasonably in light of the nature of the personal information requested;
  - Limiting the request response scope to only personal information collected, sold, or disclosed in the past 12 months;
  - Only permitting a maximum of two requests in a 12-month period.
- After receiving a Verified Consumer Request for access and reasonably confirming the consumer's identity, the business must provide the consumer with:
  - The categories of PI collected about that specific individual in the 12 months preceding the request;
  - The categories of sources for that PI collected;
  - The business or commercial purposes for collecting or selling that PI;
  - The categories of third parties with whom the business shares that PI;
  - The specific pieces of PI collected;
  - If the business sold the consumer's PI or disclosed it for a business purpose, two separate lists disclosing PI:
    - sales, by category of personal information and by category of third-party recipient, identifying the personal information categories that each recipient category obtained in the previous 12 months; and
    - disclosures for a business purpose, by category of personal information and by category of recipient, identifying the personal information categories that each recipient category obtained in the previous 12 months.
- The CCPA also sets specific timeframes and other requirements for responding to these information requests.

# CCPA's Deletion Rights

Consumers have the right to request that a business and its service providers delete their personal information, subject to certain exceptions.

A business may deny a verified deletion request when it must maintain the consumer's personal information to do any of the following:

1) complete the transaction for which the business collected the personal information;

2) fulfill the terms of a written warranty or product recall conducted under federal law;

3) provide a good or service requested by the consumer or reasonably anticipated within the business's ongoing business relationship with the consumer; or

4) otherwise perform a contract between the business and the consumer.

5) Detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity, or prosecute those responsible for that activity.

6) Debug to identify and repair errors that impair existing intended functionality.

7) Exercise a legal right, including exercising or ensuring free speech rights.

8) Comply with the California Electronic Communications Privacy Act

9) Engage in public or peer-reviewed scientific, historical, or statistical research in the public interest if: a) the research adheres to all other applicable ethics and privacy laws; b) deleting the personal information is likely to make the research impossible or seriously impair it; and c) the consumer provided informed consent during the initial data collection.

10) Enable internal uses reasonably aligned with the consumer's expectations based on the consumer's relationship with the business.

11) Comply with a legal obligation.

# BUSINESS OBLIGATIONS UNDER CCPA

- To comply with the CCPA, a business should:
- Make required disclosures using a privacy policy
  - Privacy Policy Required Elements;
  - Notice of Right to Opt-Out;
  - Notice of financial incentives.
- Establish processes and procedures to response when consumers exercise their CCPA rights, including employee training programs;
  - Provide Consumers with at least two methods to request information regarding PI collected, sold or disclosed;
  - Comply with a verifiable consumer request;
  - Respond to a verified consumer request in a useable format to enable Consumer to transmit the information from one entity to another entity without hindrance.
  - Respond within 45 days of receipt (which might be extended once for another 45 days if notice is received within 45 days).
  - Inform the consumer for not acting;
  - Provide the information free of charge, unless request is manifestly unfounded or excessive;
  - Delete and direct any third party service provider to delete any PI collected about the consumer, after receipt of a verified consumer request or determine if an exception applies.
  - A business cannot require that a Consumer open an account to submit verified consumer requests; but businesses can require existing account holder to submit requests through that account.
- Protect PI;
- Review service provider and third-party PI data sharing contracts for alignment with the CCPA's requirements.

# CCPA ENFORCEMENT

- CAG has Regulator and Enforcement Authority.
- On October 10, 2019, the CAG released the final regulations and announced that Compliance with CCPA began on January 1, 2020. Enforcement begins on July 1, 2020.
- Particular focus on: 1) Companies who handle large amounts of consumer sensitive, critical data, such as health records and SSNs; and 2) the 'opt-in' requirement for parents of children under 13 and teenagers, themselves, between 13-16 years old.
- Consumers may begin making requests under the CCPA and sue under the statute's narrowed private right of action as of January 1, 2020.

**Administrative Penalties for Non-Compliance**

- The CAG must give violators Notice of the alleged violation and at least 30 days to cure. If the business does not or cannot cure the violations, the CAG may seek civil penalties up to $2,500 per violation or $7,500 per intentional violation.
- These penalties extend to each affected individual and could result in large aggregate fines. Fine proceeds are deposited into a new Consumer Privacy Fund, which offsets State Court's and CAG's costs of enforcement.

# CCPA's Private Right of Action

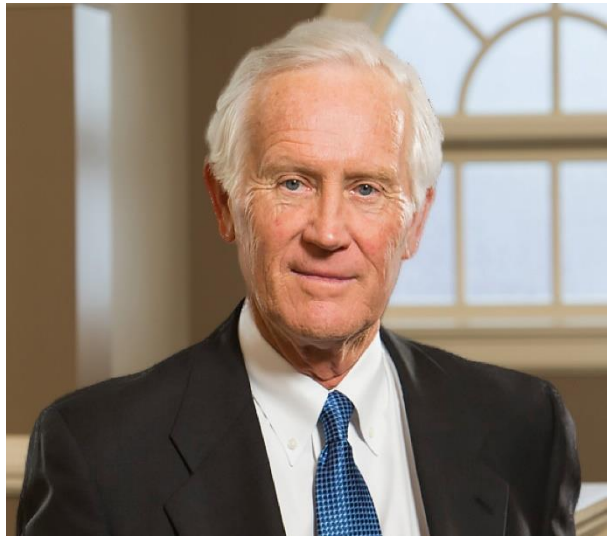
- CCPA extends the current landscape for data breach liability under CA's Data Privacy Act (CDPA). So, the CCPA's private right of action is connected to the CDPA's private right of action for unauthorized access, theft, or disclosure of non-encrypted and nonredacted PI due to the business failing to implement reasonable security practices and procedures appropriate for the type of PI.
- The potential damages in a private right of action include: statutory damages between $100-$750 per CA resident and per incident, or actual damages whichever is greater; injunctive or declaratory relief or any other relief a court deems proper.
- Statutory damages may only be available if, before filing a data breach lawsuit:
  - the consumer provides the business with a written notice identifying the specific CCPA violations and a 30 day period in which to cure the violation(s), if possible; or,
  - the business does not (or cannot) cure the alleged violation and does not provide the consumer with an express written statement within the 30 days stating that it cured the violation and that no further violations will occur.
- If the business continued with its alleged violations, the consumer can file a lawsuit request statutory damages for the original violation, and any new CCPA violation after the notice, including breaching the written statement.

# Employee Benefits Update

By:

N. Thomas Horton – nth@barrettlaw.com

Steve R. Uhey – sru@barrettlaw.com



# N. Thomas Horton

## Senior Counsel

**Phone: 260-423-8830**
**Fax: 260-423-8920**
**Email: nth@barrettlaw.com**

Tom focuses his practice in the areas of ERISA and employee benefits, including counseling clients on the design, drafting, and compliance issues pertaining to qualified retirement plans, 403(b) plans, non-qualified plans, and the ACA. Tom represents employers of all sizes, from small closely held employers to large employers with their headquarters in Northeastern Indiana. Tom represents both for-profit employers and non-profit employers.

Tom regularly presents speeches and seminars on employee benefit topics locally and regionally. Listed as an AV® Preeminent* rated attorney based on Martindale-Hubbell's peer review ratings, Tom has also been selected for inclusion in the *Best Lawyers of America*® publication and the *Super Lawyers*® publication in the area of Employee Benefits/ERISA. He is a member of the Allen County Bar Association, Cancer Services of Northeast Indiana Board of Directors and the Mad Anthonys Children's Hope House Advisory Board. He is past a member and president of the board of directors of the ASPPA Benefits Council of Northern Indiana.



1876

# Steve R. Uhey

## Associate

**Phone: 260-423-8878**
**Fax: 260-423-8920**
**Email: sru@barrettlaw.com**

Steve Uhey focuses his practice in the areas of employee benefits, corporate law, and business transactions. He assists clients with retirement plans, health and welfare plans and executive compensation. He also works with businesses of all sizes handling their corporate legal and governance matters and assisting with business transactions.

He is a member of the Allen County and the Indiana State Bar Associations. Prior to joining the firm, he co-founded, managed, and then later sold an e-commerce business. He also spent a summer interning for the Honorable Theresa L. Springmann for the United States District Court, Northern District of Indiana.

Steve received his B.A., from Huntington University and received his J.D., *cum laude*, from the University of Notre Dame Law School where he was a member of the Business Law Society and the Tax Clinic where he represented clients in disputes with the IRS.

# This employee benefits update will discuss the following topics:

I. New health and welfare plan rules resulting from COVID-19.

II. New retirement plan rules resulting from COVID-19.

III. Selected Non-COVID-19 developments re retirement plans and health and welfare plans.

# I. New health and welfare plan rules resulting from COVID-19

# Family's First Act (3/18/20) and CARES Act (3/27/20)

- Coverage of diagnostic testing for COVID-19
  - Required
- Inclusion of certain over-the-counter medical products without a physician's prescription and menstrual as qualified medical expenses
  - Permitted
- Telehealth Services – HDHP can cover telehealth services without a deductible and still be HSA compliant.
  - Permitted

# Guidance re High Deductible Health Plans

- A high deductible health plan is still HSA compliant even though it provides no cost coverage of:
  - COVID-19 diagnostic testing
  - Telehealth services

# New Rules re Outbreak Period

Important guidance was introduced centering around what is called the **Outbreak Period**.

- The Outbreak Period started March 1, 2020 and will end 60 days after the announced end of the current National Emergency.
- For example, if the National Emergency ended August 31, 2020 the Outbreak Period would expire 60 days from that date or October 30, 2020.

The normal deadlines with regards to the below are paused during the Outbreak Period:

1. The HIPAA notice rules re special enrollments.
2. The COBRA timeframes.
3. The claims procedure deadlines.
4. Good faith test re normal deadlines to furnish various ERISA notices and documents, including the time to remit employee contributions and loan payments.

# Guidance Ending With 2020 Plan Years

The following guidance does not turn on the end of the Outbreak Period as does the guidance discussed above. The following guidance ends with 2020 plan years. Also, the following new rules are **voluntary** on the part of the employer:

- Health Plan Mid-Year Elections re Temporary New Special Enrollment Rules – An employer can elect to amend its 125 cafeteria plan to offer some or all of the following temporary changes to the current employee election rules re enrollment in the employer's health plan:
  - Revoke an existing election that the employee made at open enrollment, to allow the employee to change his/her initial enrollment decision and enroll in another plan offered by his/her current employer.
  - Newly elect coverage on a prospective basis if the employee initially declined employer sponsored coverage at open enrollment.
  - Allow an employee to drop health plan coverage, but only if the employee attests in writing that they have other comprehensive coverage or will immediately get coverage through a spouse or the marketplace.

# Guidance Ending With 2020 Plan Years (cont'd.)

- Health FSA and DCAP: An employer can choose to offer some or all of certain new temporary employee election rules, such as revoking a current election, making a new election, or the increase/decrease of an existing election.
- Grace Period: This guidance allows 125 plans who use the grace period technique, to extend the grace period to December 31, 2020.
- Carryover Provisions: The guidance increases the carryover amount to $550 (from $500) for 125 plans who use the carryover technique. Also, the $550 amount is now indexed.

# The Following New Rules are Permanent and Do Not Have an Expiration Date Based Upon COVID-19

- Qualified medical expenses can include over the counter drugs without a prescription and menstrual products.
- The new Section 125 carryover amount for 125 plans who use the carryover technique (which was increased from $500 to $550 and which amount is now indexed).

# II. New retirement plan rules resulting from COVID-19

# The CARES Act Impact on Defined Contribution Retirement Plans

- The CARES Act was signed by President Trump on March 27, 2020.
- Significant provisions:

1. Participant withdrawals of a coronavirus-related distribution.
    - Pertains to withdrawals made by 12/30/20.
2. Increased participant plan loan limits.
    - Pertains to loans taken by 9/22/20.
3. Suspension of loan repayments.
    - Pertains to loan payments due by 12/31/20.
4. Waiver of 2020 RMDs.

# During the Outbreak Period – Potential Relaxation of Certain Deadlines

- The normal deadline to accomplish certain ERISA notices and documents are replaced by a good faith test to accomplish as soon as is administratively practical. This also applies to good faith failure to timely remit employee contributions and loan payments.
- Definition of Outbreak Period – See the slides pertaining to health and welfare plans.

# IRS Guidance re Terminating/Suspending Employer Contributions Mid-Year.

- Due to COVID-19's impact on employers, there has interest by some employers in terminating/suspending the employer matching contribution and/or employer non-matching contribution that the employer would otherwise make during the 2020 plan year.
- In addition to certain regulatory pre-conditions pertaining to this topic, on 6/29/20 the IRS issued Notice 2020-52 which relaxed the "normal" rules with regards to the suspension or reduction of safe harbor contributions. However, to take advantage of these relaxed rules, a plan amendment needed to be adopted by August 31, 2020.

# III. Selected Non-COVID-19 developments re retirement plans and health and welfare plans

# Retirement Plans

- SECURE ACT (signed 12/20/19)
  - Multiple Employer Plans / Pooled Employer Plans
    - For the first time, so-called "open" MEPs (now called Pooled Employer Plans or "PEPs") are permitted. This means that unrelated employers can join together a 401(k) or a 403(b) plan, even though they have no commonality between them. Prior to this change in the law, unrelated employers could only band together if there was some commonality to one another (such as a trade association plan).
    - This new rule may have a revolutionary effect, especially for smaller employers. Smaller employers can now band together into one plan, and potentially get certain advantages that might be available to a larger plan (such as cheaper share classes, lower administrative costs).
    - If certain rules are met, the plan would be considered as one plan for purposes of having one Form 5500, one CPA audit, etc.
    - PEPS are permitted commencing with 2021 plan years.

# Retirement Plans (cont'd.)

- Long-term part-time employees
  - Inclusion of Long-Term Part-Time Employees re Elective Deferral Contributions
    - If long-term part-time employees meet certain rules, such part-time employees are entitled to make elective deferral contributions to a plan, but they are not entitled to receive any employer contributions.
    - This new rule pertains to employees working more than 500 hours but less than 1,000 per year for three consecutive years. Years beginning before January 1, 2021 are not counted.
    - Starting with 2021 plan years, employers will need to start tracking part-time employee hours of service. Commencing with 2024 plan years, a long-term part-time employee may be permitted to make elective deferral contributions pursuant to this new rule.
  - RBD increased from age 70½ to age 72.
- Electronic Disclosures
- DOL Guidance re ESG Investments
- Fee Litigation
- Cybersecurity Matters

# Health and Welfare Plans

- New Types of HRA Plans
  - Effective as of January 1, 2020, two new types of HRAs are allowed for employers of all sizes:
    - Individual Coverage HRA ("ICHRA")
    - Excepted Benefit HRA ("EBHRA")
    - These new types of HRAs allow an employee to purchase individual health coverage with before-tax dollars.
  - This type of employer health plan would be more of a defined contribution variety, in that the employer would agree to reimburse some or all of the amount of an employee's premiums to purchase an individual health policy.
  - Some are touting these plans as revolutionary, akin to when defined contribution 401(k) plans where introduced in the retirement plan market.
- New Model COBRA Notices
- Class Action Litigation re COBRA Notices
- Health Plan Litigation