VOLUME 73 ◆ NUMBER 7

Employee Benefit Plan Review

CCPA Guide: Does Personal Information Include Employee and Employee Benefit Plan Data?

THEODORE P. AUGUSTINOS, LAURA L. FERGUSON, AND SEAN KILIAN

Beginning on January 1, 2020, the California Consumer Privacy Act of 2018 (CCPA) will impose new privacy obligations on certain businesses that collect personal information of California consumers. Employers with employees in California are trying to navigate how the CCPA applies to the employment relationship, including information related to employee benefit plans. Below is a summary of the potential implications for employers that are a "business" covered by the CCPA.[1]

ARE MY EMPLOYEES COVERED BY THE CCPA?

The definition of "consumer" is very broad, providing that any natural person who is a California resident is a "consumer" for purposes of the CCPA. Currently, this broad definition extends to cover employees who are resident in California. The fact that their relationship with the business is as an employee, and not a consumer of the goods and services of the business, is irrelevant for this purpose. Residency is determined using an analysis of whether an individual is (i) in California for other than a temporary or transitory purpose; or (ii) domiciled in California but temporarily or transitorily outside of California. Therefore, your employees who are domiciled in California, including those who are temporarily outside of California on business, are consumers under the CCPA. However, your employees who travel to California to do business periodically, but are not considered resident there, are not "consumers" under the CCPA.

Whether the CCPA will apply to consumers in their capacities as employees is in flux right now due to a pending amendment to the CCPA by AB 25, which has itself been revised since it was first introduced. A previous version of AB 25 would have modified the definition of "consumer" to exclude employees from the definition. The July 11, 2019 version of AB 25 would leave the definition of "consumer" unchanged, but it would provide a temporary respite for employers. AB 25 states that the CCPA does not apply to:

> Personal information that is collected by a business about a natural person in the course of the natural person acting as a job applicant to, an employee of, owner of, director of, officer of, medical staff member of, or contractor of that business to the extent that the natural person's personal information is collected and used by the business solely within the context of the natural person's role or former role as a job applicant to, an employee of, owner of, director of, officer of, medical staff member of, or a contractor of that business.

However, AB 25 also states that the foregoing paragraph "shall become inoperative on January 1, 2021." As such, if the July 11, 2019 version of AB 25 passes, the CCPA generally would not cover employees on January 1, 2020, but it would cover employees – and any employment-related and employee benefit plan data held by an employer – on January 1, 2021. Reportedly, the exemption for employees may be made permanent by later amendment, but the temporary reprieve was the result of a political compromise. We cannot currently assess the likelihood of any future amendment to extend this exemption or make it permanent.

Lastly, note that under the July 11, 2019 version of AB 25, two key provisions affecting employees will come into effect with the rest of the CCPA on January 1, 2020: (1) employees can sue for data breaches; and (2) the notice regarding categories of information collected, used and disclosed by the employer must be given to the employees. Once January 1, 2021 arrives, the exemption language described above would go away and the CCPA would fully apply to consumers in their capacities as employees. The rest of this article discusses the current text of the CCPA and the implications for employment-related and employee benefit plan data.

Is Employment-Related Data Considered "Personal Information"?

Yes. As the definition of "consumer" is very broad, so is the definition of "personal information." Employment- related information is clearly "personal information" under the CCPA.[3] There is no exemption for employment- related personal information stored and maintained by an employer, unlike the privacy laws of other states, such as Texas.[4]

"Personal information" means "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."[5] Various examples applicable to the employment relationship are listed in the definition, including: name (real or alias), address, email address, SSN, driver's license number, insurance policy number, education, employment, employment history, bank account number, credit card number, or any other financial information, medical information, health insurance information, biometric information, Internet or other electronic network activity information.

Notwithstanding this definition, to the extent employment-related information is collected or used in connection with an ERISA-covered employee benefit plan, such data *may* be exempted from the CCPA due to ERISA preemption.

From an employer perspective, consider the following common types of data that would be "personal information" for purposes of the CCPA:

- New hire/onboarding paperwork, including resumes, employee applications (typically including Social Security Number, drivers' license, mailing address, and other personal information), background checks, IRS Forms W-4 (withholding), etc.;
- Payroll information, including employee bank account numbers for direct deposit;
- Credit card information provided in connection with expense reports;
- Random drug testing paperwork and results;
- Documenting of various types of leave, such as sick leave, vacation, paid time off, FMLA leave, USERRA leave, maternity/paternity leave, etc.;
- Employee benefit plans (to the extent not exempt from the CCPA); and
- Employee's online activity on a work computer/system, such as browsing history, search history, and information regarding the employee's interaction with an internet website, application, or advertisement.

Is Employee Benefit Plan Data Covered by The CCPA?

Generally, yes. Employee benefit plans collect and use personal information as the plans require various types of personal information in operation, such as name, address, Social Security Number, and insurance policy information. However, compliance obligations of certain benefit plans may be: (1) limited by the CCPA's HIPAA exemption; and (2) potentially preempted by ERISA.

1) *HIPAA Exemption*. The CCPA does not apply to "protected health information" ("PHI") of a group health plan that is a "covered entity" subject to HIPAA or to other personal information maintained by the covered entity in the same fashion as PHI.[6] Employer sponsored HIPAA-covered benefit plans typically include a major medical plan, dental, vision, health flexible spending account, and certain wellness or employee assistance programs. It is important to note that some information collected by a plan may be personal information under the CCPA, but not PHI under HIPAA, and there may be compliance obligations with respect to that information.
2) *ERISA Preemption*. ERISA-covered benefit plans that are not HIPAA-covered (such as retirement, long term disability, life, and accidental death and dismemberment) may be able to successfully argue that personal information collected and used in connection with such plans are not subject to the requirements of the CCPA. ERISA supersedes all "state laws" (including state law causes of action) that "relate

to" employee benefit plans that are covered by Title I of ERISA.[7] ERISA preempts a state law if (1) the state law imposes requirements explicitly with reference to ERISA plans, or (2) if the state law governs central matters of plan administration or that interferes with nationally uniform plan administration.[8] Although the CCPA does not explicitly reference ERISA plans, the CCPA is likely to have a direct impact on the ability of an employer to have a nationally uniform plan administration for its benefits when operating in multiple states. The CCPA would require the employer to subject the ERISA plan to employee/participant requests for access and deletion that would be likely to significantly increase the cost of operating plans with respect to California employees/participants. Unfortunately, absent guidance that may be provided by the California Attorney General, in order to find out if the CCPA is in fact preempted so compliance is not required a company may need to bear enforcement risk, and be willing to spend time and money to litigate the issue.

Most employers likely maintain non-ERISA benefit plans that would be required to comply with the CCPA, such as short-term disability (if designed as a pay practice), various types of leave/vacation/paid time off, dependent care flexible spending accounts, and voluntary insurance (such as Aflac). Therefore, employers will need to consider whether claiming ERISA preemption is worthwhile, given that some of the employer's plans may and others may not be subject to the preemption argument. In addition, many ERISA plans are administered by third party vendors that may otherwise be preparing to comply with the CCPA, which could reduce some of the challenges with compliance at least with respect to the benefit plan data held by the third party vendor.

What Rights Do My Employees Get Under the CCPA?

The CCPA gives consumers, including your employees who are residents of California, various rights related to their personal information held by your business if your business is subject to the CCPA. For employees, here is what that currently means:

- *Right to Data Access*. Employees may request categories of, and specific pieces of personal information that the employer has collected about them. The employer must promptly provide the employee with that data, upon verification of the employee's identity.
- *Right to Deletion*. Employees may request that an employer delete any personal information the employer has collected about the employee. An employer is not, however, required to comply with the request to delete when it is necessary for the employer to maintain the personal information in certain situations.[9]
- *Disclosure Requirements*: Upon verified request, the employer must provide to an employee the:
  - Categories of personal information collected;
  - Categories of sources from which personal information is collected;
  - Purpose for collecting such information;
  - Categories of third parties with access to the personal information; and
  - Specific pieces of personal information collected about the employee.[10]
- *Right to Opt-Out*. Although a consumer has the right to opt out of a businesses' sale of the consumer's personal information to third parties, this is unlikely to come up in the context of the employment relationship as employers typically do not "sell" employees' personal information.[11]

What Key Steps Should Employers Take?

An employer subject to the CCPA should apply the same steps it is applying to "personal information" it collects from customers and other consumers to employee data and employee benefit plan data that may be subject to the CCPA. However, as a practical matter, the notices provided and the processes involved may be communicated and operated differently for the employee population versus external "consumers."

A few key issues for employers include:

- Determine which employees are residents of California or whether to extend the California consumer rights to all employees.
- Determine whether employee benefit plan data is personal information that is not exempt from the CCPA.
- If your business is a "covered entity" under HIPAA and/or the CMIA,[12] determine whether employee data is subject to the same privacy and security protections as patient information.
- Determine which systems and third party service providers hold the employee information.
- Develop a streamlined method by which employees can make personal information access and deletion requests.
- Develop processes to identify and isolate an individual's information.

- Train a team of employees to handle and respond to CCPA requests from employees.
- Employers subject to the CCPA should begin compliance efforts immediately in order to be prepared for the onerous requirements in advance of the CCPA effective date of January 1, 2020.

Notes

1. *See*, "Are You Covered by the CCPA?," at *https://www.lockelord.com/newsandevents/publications/2019/01/locke-lord-quickstudy-ccpa-guide*.
2. California Code of Regulations, Title 18, Section 17014.
3. CCPA Section 1798.140(o)(1)(I).
4. For example, in Texas, the medical records privacy law provides an exemption for employers, except with respect to a limited provision on the prohibition on reidentification of PHI. Texas Health and Safety Code Section 181.051.
5. CCPA Section 1798.140(o)(1). Note that "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.
6. CCPA Section 1798.145(c)(1)(A) and (B).
7. ERISA Section 514(a).
8. Shaw v. Delta Air Lines, Inc., 463 US 85 (1983).
9. CCPA Section 1798.105.
10. There are additional disclosure requirements if an employer sells employee information for a business purpose; however, a typical employer would not be selling employee information and such disclosure requirements are not discussed herein. CCPA Section 1798.115.
11. CCPA Section 1798.120.
12. CCPA Section 1798.145(c)(1)(B).

Theodore P. Augustinos is a partner at Locke Lord LLP advising clients in various industries on privacy and data protection, cybersecurity compliance and incident preparedness, and breach response. Laura L. Ferguson is a partner at the firm, where she assists clients with a wide variety of employee benefits, executive compensation, and privacy and cybersecurity matters. Sean Kilian is a counsel in the firm's Dallas office where he focuses his practice on labor and employment law and privacy and data security law. The authors may be reached at *ted.augustinos@lockelord.com*, *lferguson@lockelord.com*, and *skilian@lockelord.com*, respectively.