bankers' compliance group®

CPPA Finalizes Regulations on Cybersecurity Audits, Risk Assessments, and ADMT*

The California Privacy Protection Agency (CPPA) is responsible for administering and enforcing the California Consumer Privacy Act (CCPA). The CPPA is required to issue regulations addressing the following topics: (i) the circumstances under which businesses must perform an annual cybersecurity audit (including the scope of those audits); (ii) the requirements for when a business must submit a privacy risk assessment (PRA) to the CPPA on a regular basis, and the scope of the risk assessment (collectively, the "PRA Requirements"); and (iii) the access and opt-out requirements when a business uses "automated decision-making technology" ("ADMT Requirements").

As previously reported to BCG Members, on November 22, 2024, the CPPA issued a notice of proposed rulemaking addressing the cybersecurity audit, PRA Requirements, and ADMT Requirements (the "Proposed Regulations"). For a detailed discussion of the Proposed Regulations, institutions can refer to BCG Handout #25-01A, "CCPA November 2024 Proposed Regulations: Cybersecurity Audits, ADMT and Privacy Risk Assessments" (January 2025).

Since the Proposed Regulations were issued, the CPPA has held multiple board meetings to debate and refine various aspects of these regulations. While it was not clear when these regulations would be issued in final form, on September 23, 2025, the CPPA announced that the California Office of Administrative Law had approved final regulations covering cybersecurity audits, PRAs, and ADMT Requirements (the "Final Regulations"). The Final Regulations are set to take effect on January 1, 2026. However, the Final Regulations provide businesses with extended deadlines to comply with its requirements. A summary of some of the critical requirements in the Final Regulations is provided below.

Cybersecurity Audits

The Final Regulations address the circumstances under which a business must conduct a cybersecurity audit and the scope of such audit into new Article 9 of the current CCPA regulations (11 CCR Section 7120 *et seq.*) Under the Final Regulations, a business is required to conduct a cybersecurity audit if its processing of personal information (PI) presents significant risk to consumers' security. The Final Regulations clarify that processing PI presents a significant risk to security if any of the following conditions are met:

* Janet Bonnefin has retired from the firm.

- The business derives 50 percent or more of its annual revenues from selling or sharing PI; or

- The business had annual gross revenues exceeding $26,625,000 in the preceding calendar year; and

    - Processed the PI of 250,000 or more consumers or households during the prior calendar year; or

    - Processed the sensitive PI of 50,000 or more consumers in the prior calendar year. 11 CCR Section 7120(b)(1)-(2).

If a business meets any of the above thresholds, it must conduct an annual cybersecurity audit that satisfies the requirements set forth in Article 9 (see 11 CCR Section 7122; 7123; & 7124).

***Compliance Deadline Cybersecurity Audits*.** While the regulations go into effect on January 1, 2026, the Final Regulations provide businesses additional time to complete the cybersecurity audits required by Article 9. A business subject to Article 9 would need to complete its first cybersecurity audit report by no later than one of the following dates, as applicable:

- **April 1, 2028**: If the business's annual gross revenues exceed $100 million for 2026 (as of January 1, 2027), the audit would need to cover the period from January 1, 2027 through January 1, 2028.

- **April 1, 2029**: If the business's annual gross revenues are between $50 million and $100 million for 2027 (as of January 1, 2028), the audit would need to cover the period from January 1, 2028 through January 1, 2029.

- **April 1, 2030**: If the business's annual gross revenues are less than $50 million for 2028, the audit would need to cover the period from January 1, 2029 through January 1, 2030.

- **After April 1, 2030**: After April 1, 2030, any business that meets the criteria discussed above on January 1 of a given year (based on the preceding calendar year) must complete a cybersecurity audit covering the next 12 months. The audit report would then need to be completed by April of the following year.

Privacy Risk Assessments (PRAs)

The Final Regulations also require businesses whose processing of PI presents a significant risk to consumers' privacy to conduct a PRA before initiating that type of processing. For example, using ADMT to make a significant decision regarding a consumer or for extensive profiling would trigger the PRA requirement. Notably, the term "significant decision" is defined to include, among other things, decisions that result in access to, or the provision or denial of, financial or lending services. Therefore, financial institutions that use ADMT to provide or deny access to financial services would likely be required to conduct a PRA. The Final Regulations also describe the scope of the PRA that businesses would be required to conduct.

***Compliance Deadline PRAs*.** While the regulations go into effect on January 1, 2026, the Final Regulations give businesses additional time to complete and submit their PRAs to the CPPA. Businesses must begin completing PRAs on January 1, 2026. However, any business subject to the PRA requirements has until April 1, 2028 to submit PRAs completed in 2026 or 2027 to the CPPA.

ADMT Pre-use Notice Requirements

Any business that uses ADMT for certain reasons (enumerated in CCR Section 7200) must provide consumers with a notice that describes: (i) the consumer's right to opt out of ADMT; (ii) how the business will use ADMT; and (iii) the consumer's right to access information about the business's use of ADMT (collectively, the "Pre-use Notice"). Notably, using ADMT in connection with a decision that results in access to, or the provision or denial of, financial or lending services seems to trigger the Pre-Use Notice requirements.

***Compliance Deadline ADMT Pre-use Notice*.** While the regulations go into effect on January 1, 2026, the Final Regulations provide businesses additional time to comply with the Pre-use Notice requirements. Businesses must be in compliance with the Pre-use Notice requirements no later than January 1, 2027.

The Final Regulations can be found on the CPPA's website at: **https://cppa.ca.gov/regulations/ccpa_updates.html**.

For more information, contact John Davis at **JDavis@ABLawyers.com** or Keith Forrester at **KForrester@ABLawyers.com**.