MAYER | BROWN

CCPA CYBERSECURITY AUDIT REGULATIONS:
WHAT BUSINESSES NEED TO KNOW

PRESENTING TODAY

PARTNER
CYBERSECURITY & DATA PRIVACY

STEPHEN LILLEY

WASHINGTON DC +1 202 263 3865
NORTHERN CALIFORNIA +1 415-874-4273
SLILLEY@MAYERBROWN.COM

PARTNER
CYBERSECURITY & DATA PRIVACY

LEI SHEN

CHICAGO +1 312 701 7270
LSHEN@MAYERBROWN.COM

AGENDA

1. Background and scope of cybersecurity audit requirements
2. Requirements for audits and auditors
3. Key risks
4. Priorities for CCPA audit readiness

BACKGROUND

- California law requires businesses to "maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information [about California residents] from unauthorized access, destruction, use, modification, or disclosure."
- In support of that goal, the amendments to the CCPA regulations finalized by the California Privacy Protection Agency (CalPrivacy) in September 2025 require that businesses processing a sufficient volume of Californians' personal information must complete **independent audits of their cybersecurity programs**.
- Responsible executive must submit **certification of compliance** to CalPrivacy annually.
  - Must represent that the "business has not made any attempt to influence the auditor's decisions or assessments regarding the cybersecurity audit."
- Largest businesses must complete the first audit reports by **April 1, 2028,** covering the **year beginning on January 1, 2027**.

BUSINESSES IN SCOPE

- CCPA cybersecurity audit regulations apply to each business whose "processing of consumers' personal information presents **significant risk** to consumers' security"
  - Derive 50% or more of annual revenue from selling or sharing personal information;

    OR
  - Gross revenue over $25 million (as adjusted over time) AND in past year either:
    - Processed personal information of 250,000 or more consumers, OR
    - Processed the sensitive personal information of 50,000 or more consumers
- Note that "consumers" essentially means any individual in California
- Consider CCPA exceptions
- Reporting deadlines vary based on business size:
  - By April 1, 2028 if business makes over $100 million
  - By April 1, 2029 if business makes between $50 million – $100 million
  - By April 1, 2030 if business makes less than $50 million

AUDITOR REQUIREMENTS

- Must use a qualified, objective, independent professional auditor using procedures and standards accepted in the profession of auditing
  - Must have knowledge of cybersecurity and how to audit a cybersecurity program
  - Must be impartial and free to make decisions without being influence by the business being audited
- The auditor must receive all information that the auditor requests as relevant to the cybersecurity audit
- May be internal or external; if internal, auditor must not report to an executive with direct responsibility for the business' cybersecurity program

AUDIT REQUIREMENTS

- Assessment of cybersecurity program in light of the business's size and complexity and nature and scope of its processing activities
- Auditor determines the scope of audit and criteria to be used
- Assessment of at least eighteen listed program components – but may go further. These include:
  - *Authentication (MFA, passwords)*
  - *Encryption of personal information*
  - *Account management and access controls*
  - *Inventory and management of personal information and information systems*
  - *Secure configuration of hardware and software*
  - *Vulnerability scans, PEN testing, and vulnerability disclosure and reporting*
  - *Cybersecurity awareness*
  - *Cybersecurity education and training*
  - *Secure development and coding best practices*
  - *Oversight of service providers, contractors, and third parties*
  - *Retention schedules and disposal of personal information*
  - *Incident response management*
- The resulting audit report must document any "gaps or weaknesses" that "increase the risk of" unauthorized activity relating to personal information, as well as the business' plan to address these gaps or weaknesses
- Annual certification of completion must be made, under penalty of perjury, and submitted to CalPrivacy

KEY RISKS

- Creation of unprivileged and thorough report describing weaknesses in cybersecurity program
- Potential for distortion of sound, risk-based approach to cybersecurity
- Direct compliance challenges and cost associated with an independent and expansive audit with an indefinite measuring stick
- Required certification under penalty of perjury

PRIORITIES FOR CCPA CYBERSECURITY AUDIT READINESS

Coverage

Applicability

- Which entities are subject to the regulation?
- When must first audit(s) be performed?

Scope

- What systems hold personal information of California residents?
- What other systems should be brought into the audit?

Process

Auditor Selection

- Who will perform the audit?
- What can be known about auditor's approach?
- Will company rely on prior audits?

Executive Selection

- Which executive will make necessary certifications?
- What internal processes will support required certifications?

Readiness

Assessment

- What should be assessed?
- Who will perform assessment?
- How should assessment be performed?

Remediation

- What steps will be taken to enhance program maturity?
- What resources will be necessary to support these steps?