SW&M FINANCIAL INSTITUTION ATTORNEYS

Compliance Alert

CALIFORNIA APPROVES NEW CCPA REGULATIONS ON AUTOMATED DECISION-MAKING, RISK ASSESSMENTS, AND CYBERSECURITY AUDITS

Overview

In July 2025, the California Privacy Protection Agency (CPPA) finalized a significant package of regulations under the California Consumer Privacy Act (CCPA), covering automated decision-making technology (ADMT), risk assessments, and cybersecurity audits. These rules, approved on July 24, 2025, are now before the Office of Administrative Law (OAL) for review. The OAL is expected to issue a decision by mid-September 2025 (with the possibility of an extension into November). Once effective, these regulations will impose substantial new compliance obligations across industries. For financial institutions—banks, credit unions, and other consumer-facing lenders—the rules are particularly impactful given the reliance on automated systems for credit underwriting, fraud prevention, and digital member and customer engagement.

1) **Automated Decision-Making Technology: New Duties of Transparency and Control**

Automated tools are becoming more prevalent to how financial institutions make decisions. Banks and credit unions are beginning to use ADMT for loan approvals, credit scoring, fraud detection, and other purposes to serve their customers. Under the new regulations, such uses will require clear, accessible disclosures whenever automated processing materially affects a consumer's access to financial products or services, unless an exception applies.

Institutions must explain that automation is being used, describe the logic at a high level, and disclose the potential consequences of the decision. In certain contexts, consumers must also be offered the ability to opt out or request meaningful information about how their data contributed to an outcome. These provisions are expected to take effect on January 1, 2026, and will require updates to privacy notices, customer-facing portals, and internal workflows for responding to consumer inquiries.

Agreements with vendors that use ADMT in providing services to members or customers must be revised to incorporate contracts clauses requiring the vendor to comply with ADMT regulations and cooperate with the financial institution in connection with consumer opt-out and other rights concerning the use of ADMT.

2) Risk Assessments: Structuring High-Risk Data Practices

The regulations also introduce detailed requirements for risk assessments in connection with high-risk processing, including the use of sensitive personal information, large-scale profiling, or reliance on ADMT.

Financial institutions will need to conduct formal assessments that weigh the benefits of the data practice against the potential risks to privacy, security, and civil rights. The assessments must also document safeguards to mitigate those risks. Importantly, these are not merely internal exercises—the CPPA requires submission of assessments on a periodic basis beginning in 2027–2028. This expectation means institutions must develop repeatable, documented processes for evaluating new products, technologies, and vendor arrangements.

3) Cybersecurity Audits

Finally, the regulations establish a regime for independent cybersecurity audits. Large institutions and those engaged in high-risk processing will be required to undergo recurring audits of their security programs, conducted either internally by a sufficiently independent function or externally by a qualified auditor.

The audits must evaluate whether security measures are not only properly designed but also operating effectively in practice. For financial institutions, this will extend beyond technical safeguards like encryption and multifactor authentication to include vendor oversight, incident response, and governance structures. Audit obligations begin on January 1, 2027, with the first reports due between 2028 and 2030, depending on the size and activities of the institution.

4) Implications for Financial Institutions

The new regulations signal a shift in California toward active regulatory oversight of how institutions use data and technology in serving consumers. For banks, credit unions, and other lenders, the rules are especially significant because they touch the core of financial decision-making processes.

- **Transparency**: Institutions will need to explain how algorithms and automated tools influence credit, fraud, and service outcomes.
- **Accountability**: Risk assessments will require institutions to justify their data practices in a structured and reviewable way.
- **Governance**: Cybersecurity audits will bring independent scrutiny to longstanding information security practices.

These obligations echo global trends, including the EU's AI Act and U.S. federal discussions around algorithmic accountability. Early preparation will not only reduce compliance risk but also reinforce consumer trust—a cornerstone for financial institutions.

5) **Next Steps**

- **Map ADMT uses now**: Identify where automated decision-making tools affect credit decisions or member services. Identify potential exceptions that might apply, such as data processed pursuant to the Gramm-Leach Bliley Act ("GLBA"), and use cases where the GLBA does not apply, such as the use of ADMT in the employment context or with respect to business accounts and loans.
- **Review notice procedures**: Update privacy notices to anticipate 2026 requirements.
- **Develop risk assessment frameworks**: Begin aligning with CPPA expectations before 2027 deadlines.
- **Plan for cybersecurity audits**: Credit unions should evaluate whether to engage external auditors early.
- **Vendor engagement**. Identify vendors that may be using ADMT to provide services for your organization and update contracts with such vendors to address additional compliance requirements.

6) **To support compliance, SW&M is making available:**

To support clients in navigating these requirements, SW&M has developed a comprehensive set of compliance tools and advisory services. These include model policies, such as updated CCPA privacy policies and pre-use notices addressing ADMT disclosures; template risk assessment forms designed specifically for financial institutions; and advisory sessions tailored to help organizations assess the scope and applicability of the regulations, while addressing institution-specific questions.

SW&M's Privacy & Cybersecurity Practice Group is closely monitoring OAL's review process and will issue updates as the regulations move toward effectiveness.