The California Consumer Privacy Act (CCPA) – What RIAs and Fintechs Need to Know

The California Consumer Privacy Act (CCPA) requires all businesses that collect personal information from California customers or clients to adhere to the nation's most stringent data privacy laws and guarantee customers' rights to control their personal information.

The penalties for not complying with the CCPA are steep: the California Attorney General may fine investment advisors, broker-dealers, and fintechs $2,500 **per violation** (even if the violation was accidental) and $7,500 **per violation** (if intentional). Fintechs and RIAs also face civil lawsuits under the private right of action rule in the CCPA, which gives California residents the right to sue your company or firm for not following the law.

Costs can rack up quickly. If you're found violating the CCPA with twenty customers, you could be looking at $50,000 in penalties before any civil litigation.

If you have just one customer in California, compliance with CCPA is mandatory. Even if you're not domiciled in California, you must still comply with the law if you market or sell products in California, work with independent contractors in the state, or do any business there.

What is considered personal information under the CCPA?

Pretty much anything and everything. For example, email addresses and names are considered protected personal information under the CCPA. This law goes beyond simply safeguarding "sensitive information" (social security numbers, account logins, etc.) that could harm customers. Any personal information you collect from California customers exposes your company or firm to significant regulatory penalties and lawsuits if mismanaged.

What are the compliance requirements under the CCPA?

Under the California Privacy Rights Act (CPRA) of 2020 or CCPA 2.0, compliance requirements include:

- Limiting the disclosure of sensitive information to third parties
- Giving customers or clients the right to opt out of sharing or selling personal information
- Ensuring personal information is accurate
- Deleting personal information on request

- Correcting inaccurate data and personal information on customers or clients

Does sharing personal information with subcontractors or service providers pose a threat?

Yes. RIAs and fintechs that grant subcontractors or service providers access to the personal information of their California customers or clients require contracts with terms and provisions that:

- Specify the limitations and purposes in the disclosure of personal information
- Obligate the subcontractor or service provider to comply with the CCPA
- Grant companies the right to confirm that service providers comply with the CCPA
- Require third parties to inform companies if they can't meet CCPA obligations
- Give companies the ability to remedy third-party CCPA non-compliance

Sound third-party risk management, particularly contract management, plays a vital role in protecting RIAs and fintechs from legal liability and regulatory penalties under the California Consumer Privacy Act, which amended and expanded the CCPA in 2020 (with most provisions taking effect in 2023).

How to comply with state regulatory requirements outside your territory

If you conduct business or have any customers located in California, you must comply with the CCPA. RIAs and fintechs that operate nationally or do business in various states must also comply with all separate state regulatory requirements.

With the help of a state regulatory requirements builder, companies ensure compliance with state regulations, avoiding costly penalties and potential lawsuits. They can also assess if the expected revenue from expanding their business into new states is worth the compliance cost.

RIAs and fintechs with California customers (or those that conduct any extra-territorial business) need a robust vendor risk management program and compliance management system.

About Nvendor
Ncontracts' Nvendor is a comprehensive vendor management software solution that streamlines and automates the entire vendor lifecycle, from due diligence and risk assessment

to ongoing monitoring and performance management, empowering organizations to efficiently manage third-party relationships while promoting compliance and reducing risk.