https://fdata.global/

February 26, 2026

California Department of Financial Protection and Innovation
Legal Division, Regulations Coordinator
Attn: Diana Pha
651 Bannon Street, Suite 300
Sacramento, CA 95811

Re: PRO 07-24 Second Invitation for Comments on Proposed Rulemaking under the California Consumer Financial Protection Law Regarding Registration and Reporting of Covered Persons (Consumer-Reporting Services)

Dear Commissioner Khalil "KC" Mohseni and Department Staff,

The Financial Data and Technology Association ("FDATA") appreciates the opportunity to provide comments on the Department of Financial Protection and Innovation's ("DFPI" or "the Department") second invitation for input regarding potential registration and reporting requirements for persons that provide the consumer financial service described in Financial Code Section 90005(k)(9). FDATA's primary concern is that the breadth of any implementing framework should not impede consumers' ability to access and permission the sharing of their financial data held by financial institutions, a right enshrined in federal law under Section 1033 of the Dodd-Frank Wall Street Reform and Consumer Protection Act ("Dodd-Frank Act").

As written, the covered activity description in Section 90005(k)(9) is not sufficiently precise to distinguish between (i) consumer-permissioned services that transmit account information at a consumer's express direction as federally protected under Section 1033 of the Dodd-Frank Act; and (ii) consumer reporting activity that assembles information for eligibility determinations under established federal frameworks. That lack of precision is the central problem: it risks attaching registration and reporting obligations to the wrong activities and the wrong entities, which could reduce consumer access to everyday financial tools or create parallel state-level registration, reporting, and supervisory obligations for activities already comprehensively governed under federal consumer-reporting law.

California has long been a leader in consumer financial protection and a center of technology-driven innovation that advances transparency, competition, and consumer choice. With that history in mind, our comments focus on ensuring that any registration and reporting regime intended to address non-permissioned collection, or use, does not inadvertently cover consumer-permissioned tools and services that operate only at the express direction of the consumer, such as budgeting, personal financial management, account monitoring, payment initiation, pay-by-bank, income and cash-flow verification

https://fdata.global/

(including underwriting use cases), overdraft avoidance, and other fee-avoidance services that operate under a statutorily mandated process pursuant to Section 1033 under the Dodd-Frank Act. At the same time, where consumer-permissioned data is assembled for use in credit decisioning within a framework governed by the Fair Credit Reporting Act ("FCRA"), those activities are already subject to comprehensive federal regulation, including requirements relating to dispute resolution and complaint handling. Any state-level framework should recognize these existing guardrails and avoid creating conflicting or duplicative standards. However, as currently drafted, the proposed regulation runs the risk of limiting access to these tools and creating uncertainty regarding how FCRA-regulated entities would be treated under the California Consumer Financial Protection Law ("CCFPL").

FDATA's members support strong consumer protections and share DFPI's goal of preventing practices that could harm consumers or distort the marketplace. At the same time, effective regulation depends on clear, administrable lines that attach regulatory obligations to the right activities. As currently framed, Financial Code Section 90005(k)(9) is broad, describing "collecting, analyzing, maintaining, or providing consumer report information or other account information" when "used or expected to be used in connection with any decision regarding the offering or provision of a consumer financial product or service."[1] The scope of those activities and the ambiguity around key terms create a real risk that the Department's proposed registration and reporting regime could be applied to entities that are enabling consumers and small businesses to exercise their statutory rights under Section 1033 to access, review, and share elements of their financial data—at their express direction—with financial tools and services that can improve their financial well-being, and that do not themselves determine eligibility, extend credit, or control downstream credit decisions.

DFPI can address that risk by adopting a function-based approach that distinguishes consumer-permissioned data access services—operating at the direction and with the authorization of the consumer—from other data-handling activities that appear to be the Department's focus for registration and reporting. In particular, the Department should ensure that any registration and reporting obligations are targeted to models where consumers do not affirmatively permission access to their data for a specific purpose and that such obligations do not apply to persons or activities regulated under the FCRA. Any reporting and registration requirements should be calibrated to the specific consumer and market risks presented by the activity at issue and should avoid duplicative or conflicting obligations for entities already subject to comprehensive federal oversight under the FCRA.

[1] *See* https://dfpi.ca.gov/wp-content/uploads/2026/01/PRO-07-24-Second-Invitation-for-Comments.pdf.

https://fdata.global/

I. Consumer-permissioned data access enables consumer-beneficial tools and services and should not be conflated with consumer reporting activity subject to FCRA

In discussing what acts or practices by data-handling servicers provide benefits to consumers; the Department appropriately highlights consumer outcomes as the touchstone of its analysis. In the consumer-permissioned data access context, those benefits flow directly from consumer control and transparency. These models are designed so that consumers can access and affirmatively choose to share their own account information with a third party for a specific purpose, such as verifying income, or using a personal financial management tool. This functionality, known as "open banking" or "open finance" in much of the world, can also benefit consumers by bringing the competition benefits of data portability to the market for consumer financial products and services.[2] Consumers use these services to initiate payments, avoid overdraft and nonsufficient funds fees, monitor accounts, pay off debts, and improve day-to-day financial stability.

Some consumer-permissioned platforms transmit data at the consumer's direction without assembling or evaluating that data for eligibility determinations. Other data uses involve the assembly of consumer-permissioned information for use in credit decisioning or other eligibility determinations within frameworks governed by the FCRA, including requirements relating to permissible purpose, accuracy, and dispute resolution. These structural differences are critical and should be reflected in any DFPI rulemaking.

When consumer-permissioned data is used for credit underwriting or income verification, it can support more accurate and inclusive evaluations that responsibly expand access to affordable credit for consumers who are not well served by legacy models that rely primarily on traditional credit files. Federal policymakers, including banking and consumer-protection regulators, have repeatedly recognized the potential of cash-flow underwriting—in these use cases—to responsibly expand access to credit for these consumers. [3,4,5] These approaches often reduce friction in the application and verification process and can speed time-to-decision while preserving consumer choice, because the consumer remains in control of when and how their data is shared at all times.

---

[2] An "open banking framework" refers to a regulatory structure that gives consumers and small businesses the legal right to access and share their financial data electronically with third-party providers of their choice, typically through secure APIs. In the United States, this framework is provided under Section 1033 of the Dodd-Frank Wall Street Reform and Consumer Protection Act, which requires that covered financial institutions make available to consumers, upon request, information concerning their financial products or services.

[3] *See* https://home.treasury.gov/system/files/136/Assessing-the-Impact-of-New-Entrant-Nonbank-Firms.pdf.

[4] *See* https://www.consumerfinance.gov/about-us/blog/credit-scores-only-tells-part-of-the-story-cashflow-data/.

[5] *See* https://www.federalreserve.gov/publications/2025-october-consumer-community-context.htm.

For these reasons, the Department's question regarding whether certain market segments require particular attention is especially important. Consumer-permissioned data access platforms and technology providers are not interchangeable with other data-handling activities since they function as consumer-permissioned conduits rather than as entities that determine eligibility or control dispute outcomes. Accordingly, consumer disputes regarding underlying account information must remain with the originating financial institution that maintains the relevant system of record. By contrast, where data is assembled for use in credit decisioning within a framework governed by the FCRA, eligibility determinations remain with the downstream decision-maker, and the applicable federal reinvestigation and dispute resolution framework applies. Treating these fundamentally different roles as interchangeable would misalign regulatory accountability and dilute consumer protections by assigning obligations to entities that lack the ability or legal authority to remediate alleged harm.

Rules that fail to account for this distinction risk blurring accountability, creating duplicative or mismatched obligations, and discouraging lower-risk models that are designed to maximize consumer permission, access, and visibility.

II. Definitions should be clarified to prevent overbreadth and align obligations with function and risk

The Department's second invitation asks how the definition in Financial Code Section 90005(k)(9) compares with existing federal and state definitions and how regulations might address gaps or ambiguities. The central concern is that a broad reading of Section 90005(k)(9) could sweep in consumer-permissioned entities that provide account information used in connection with decisions about consumer financial products or services. Because the statute refers to "decisions" broadly—not eligibility determinations—and to "financial products or services" broadly—not only credit—an unbounded interpretation could reach routine consumer-permissioned activity such as payment initiation or overdraft avoidance, which could inadvertently limit access for Californians to use beneficial services.

For avoidance of doubt, the Department should clarify that tools that assess or predict transaction risk—such as likelihood of payment returns or insufficient funds—without determining eligibility or making adverse consumer decisions, do not constitute covered activity under Section 90005(k)(9).

For example, payment wallets use consumer-permissioned data access tools to mitigate risk of payments sent over their systems, similar to the functionality provided by credit card networks. Specifically, consumer-permissioned data access enables payments over such wallets by confirming that the payor has sufficient funds to complete a given payment

and does not demonstrate indicia of fraud. Likewise, overdraft avoidance and fee-avoidance tools are designed to help consumers avoid unexpected expenses. In order to do this, such tools must make decisions related to consumers' balances and ability to handle a given expense. Treating these consumer-permissioned uses as trigger points for coverage would be a mismatch of function and risk. If consumer-permissioned transmission can itself trigger registration and reporting requirements, consumers will face fewer options to use everyday payment and fee-avoidance tools that improve financial stability.

Any regulation should therefore resolve the ambiguity in § 90005(k)(9) by clarifying that consumer-permissioned data portability of account information does not, by itself, trigger coverage for registration or reporting to the Department.

Clarifying key terms is essential to achieving that result. The Department should avoid defining "consumer report," "consumer report information," and "account information" in a manner that conflates technical transmission of consumer-permissioned data with already regulated consumer reporting activity under the FCRA. Clear delineation between these functions will promote accountability while avoiding regulatory duplication. Definitions should make clear that account information includes data accessed and transmitted from accounts the consumer has lawful access to, and that the transmission of such information should not, by itself, trigger inclusion under the Department's proposed rulemaking, as such an approach risks reducing access for Californians to critical financial technology tools that support their financial wellbeing.

Similarly, the Department should clarify the definition of "consumer financial product or service," particularly the phrase "provided for use by consumers." Consumer-permissioned data access tools are provided for use by consumers because they enable consumers to access, monitor, and direct the sharing of their own financial information, even when that consumer-permissioned action facilitates a downstream transaction with a third party such as a lender. Without clarification, the phrase could be misread to include consumer-permissioned platforms simply because lenders benefit from consumer-permissioned data sharing, a result that would be inconsistent with consumer protection goals designed to promote access to affordable credit.

The Department should also clarify the scope and application of exemptions and exclusions under the CCFPL as applied to other participants in the consumer-data industry. As drafted, the definition covering entities "collecting, analyzing, maintaining, or providing consumer report information or other account information" could be read to require registration of virtually any software provider involved in consumer-permissioned data flows, regardless of the role they play in eligibility determinations, or substantive decision-making. In particular, DFPI should confirm that consumer-permissioned data access platforms and technical service providers are not subject to CCFPL registration when they do not control

dispute outcomes. Given the breadth of Section 90005(k)(9), such clarification is critical to ensure that the statute is not applied in a way that captures a wide range of participants whose activities fall outside the core consumer reporting function.

III. If DFPI proceeds, requirements must be calibrated to function and fees must be tied to California credit-decisioning revenue

FDATA recognizes the Department's authority to impose registration and reporting obligations where warranted and does not oppose such requirements when they are appropriately aligned to the regulated activity. FDATA's primary recommendation is that DFPI adopt a function-based framework that distinguishes between (i) consumer-permissioned data access platforms and technology providers that operate at the consumer's direction and do not determine eligibility or control dispute outcomes; (ii) and consumer reporting activity subject to the FCRA. That approach best preserves consumer choice and avoids regulatory overbreadth and overlap. Insofar as DFPI proceeds in a manner that captures some consumer-permissioned entities with FCRA-governed arms, the Department should calibrate requirements to function and avoid imposing prohibitive fee burdens that deter market entry, slow expansion, and ultimately reduce consumer options.

In particular, DFPI should carefully consider how registration fees are assessed and how "gross income from consumer-reporting services" is defined. Where an entity engages in both consumer reporting activity and non-reporting technical services, for instance, any assessment of "gross income from consumer-reporting services" should be limited to revenue derived from federally regulated consumer reporting activity involving California residents. Revenue attributable to technical connectivity, data portability infrastructure, fraud prevention services, or non-credit use cases should be excluded. In other registration contexts, DFPI fees can be significant. Applying similar fee structures to all enterprise activities, rather than revenue tied to California credit decisioning activity, risks discouraging newer entrants from offering services in California or delaying entry until later stages of a company's lifecycle.

This point is central: if a consumer's act of permissioning data sharing for a financial tool or service could trigger registration, reporting, and fee obligations across a platform's overall revenue base, the practical effect will be to make it harder for firms to offer consumer-permissioned tools in California and harder for consumers to access them.

The downstream impact would be fewer consumer options and reduced competition, particularly for products designed to responsibly expand access to affordable credit. Federal policymakers, including banking and consumer-protection regulators, have repeatedly recognized the potential of cash-flow underwriting to responsibly expand access

to credit for consumers who are not well served by traditional credit files.[6] Regulatory fee structures that materially increase the cost of offering these tools risk reversing those gains by discouraging adoption, pushing lenders back toward bureau-only models, and leaving thin-file and no-file consumers with fewer options. If DFPI moves forward with registration, it should clarify that gross income for fee purposes is limited to revenue derived in California from use cases that implicate the registration obligations only, excluding infrastructure-only services and non-credit use cases. Where revenue is bundled or indirect, DFPI should permit reasonable, documented allocation methodologies so that fees are assessed on regulated activity rather than on aggregation or connectivity services more broadly.

Bonding and recordkeeping requirements should be limited to activities that present a clear risk of consumer financial loss. Bonding is traditionally justified where an entity holds, moves, or controls consumer funds, or where transaction reconstruction is necessary to remediate financial harm—conditions that do not apply to consumer-permissioned data access platforms. Requiring such entities to post bonds or retain expansive records would increase compliance costs without improving consumer protection outcomes. These platforms do not hold consumer funds and do not execute transactions on a consumer's behalf. Imposing bonding requirements in this context would increase compliance costs without improving consumer protection outcomes.

In some cases, imposing expansive data-retention or bonding requirements may increase security and privacy risk without improving consumer outcomes, particularly where data minimization is a core design principle. Over-retention of sensitive financial data would also run counter to California's privacy framework, including the California Consumer Privacy Act's ("CCPA") requirements that businesses disclose and adhere to specific purposes for collection and use, and avoid retaining personal information (including sensitive personal information) longer than is reasonably necessary for the disclosed purpose.[7]

More broadly, the CCPA reflects a necessity-and-proportionality principle for collection, use, retention, and sharing, and provides consumers the right to limit the use and disclosure of sensitive personal information to what is necessary and reasonably expected. These guardrails underscore why rules that incentivize retaining more data than needed can be directionally misaligned with consumer privacy objectives while increasing breach exposure.

[6] *Ibid.*
[7] *See* https://cppa.ca.gov/regulations/pdf/ccpa_statute.pdf.

The Department also asks whether the proposed regulatory action would have significant statewide adverse economic impacts or affect the expansion of businesses currently operating in California. These impacts should be evaluated through the lens of market entry and innovation rather than through the question of whether established firms will exit the state. Fixed compliance costs and regulatory uncertainty can deter new entrants from launching in California at the earliest stages or incentivize firms to delay offering consumer-permissioned products to Californians until later in their development. Over time, that dynamic can reduce competition and slow the availability of consumer-friendly tools, with downstream effects on consumer access, affordability, and choice.

To the extent registration, reporting, or fee obligations are adopted, they should be limited to activity involving California residents and California-specific revenue. Several questions in the invitation reference total business metrics, nationwide revenue, or aggregate dispute and complaint volumes. Applying such measures to entities based on non-California activity would risk creating a de facto national consumer-reporting regime through state regulation. Any reporting, fee assessment, or oversight should therefore be limited to California-resident activity to ensure proportionality, fairness, and alignment with the Department's jurisdiction.

Reasonable alternatives exist that would allow DFPI to advance consumer protection goals with greater precision and less burden. A function-based approach that distinguishes among consumer-permissioned technical transmission, and FCRA-regulated consumer reporting; clarifies key definitions; and calibrates any registration and fee requirements to the specific activity being regulated would be equally effective in achieving the purposes of the CCFPL while preserving innovation and consumer choice.

Conclusion

FDATA appreciates the Department's engagement and the opportunity to provide input in advance of any formal rulemaking. We respectfully urge the Department to implement Section 90005(k)(9) in a manner that recognizes the meaningful differences between consumer-permissioned data access and FCRA-regulated activity. A function-based approach will best advance the purposes of the CCFPL, including consumer welfare, competition, accountability, and transparency. FDATA and its members would welcome continued engagement with DFPI staff and are available to provide additional information or practical examples of consumer-permissioned use cases and operational models.

About FDATA

As the leading trade association advocating for consumer-permissioned, third-party access to financial data, FDATA's members enable millions of consumers and small businesses

to securely access and use their financial information for payments, account aggregation, personal financial management, credit underwriting, fraud prevention, and other legitimate financial services. Regardless of their business model, each FDATA member's product or service shares one fundamental and foundational requisite: it depends on the ability of a consumer to actively permission access to some component of their own financial data that is held by a financial institution.

FDATA's members work extensively with banks of all sizes, including community banks that rely on third-party platforms to facilitate consumer-permissioned data access in a secure and compliant manner.

Sincerely,

[redacted]

Steve Boms
Executive Director
FDATA