FDATA
Financial Data and Technology Association
www.fdata.global.com

August 26th, 2026

Comment Intake
Financial Sector Policy Branch
Department of Finance Canada
90 Elgin Street
Ottawa, Ontario K1A 0G5

Submitted electronically to OBBO@fin.gc.ca.

Re: Consumer-Driven Banking Regulations *Canada Gazette*, Part I, Volume 160, Number 26

The Financial Data and Technology Association ("FDATA") appreciates the opportunity to comment on the proposed Consumer-Driven Banking Regulations published in the *Canada Gazette*, Part I on June 27, 2026. Our comments are offered in the spirit of supporting the successful implementation of Canada's Consumer-Driven Banking Act ("CDBA") and advancing a competitive, secure, and consumer-focused open finance ecosystem.

FDATA is North America's leading trade association dedicated to open finance and consumer-permissioned access to financial data. Our members collectively serve 9 million Canadian consumers and small and medium-sized enterprises ("SMEs") through financial management and accounting tools, digital banking services, investment and savings platforms, affordable credit products, payment solutions, and other innovative financial services. Across North America, FDATA members provide more than 100 million consumers and SMEs with access to financial products and services, either directly or through partnerships with regulated financial institutions.

FDATA has extensive experience contributing to and supporting the design and implementation of consumer-driven finance frameworks across multiple jurisdictions. We have long supported consumer-driven banking in Canada, which was realized through the Royal Assent of the CDBA earlier this year and which represents a thoughtful and comprehensive approach informed by international experience and tailored to Canada's financial services landscape. The proposed regulations make important progress toward operationalizing the CDBA and advancing competition, innovation, consumer protection, and financial stability.

At the same time, FDATA remains concerned that smaller fintechs, startups, and small merchants may struggle to participate in and benefit from the framework if accreditation requirements and associated costs are disproportionate to the participating entity's resources, size, and risk profile. FDATA believes this outcome would be contrary to the intent and policy goals of the CDBA. Canada's consumer-driven banking framework will only achieve its full potential if responsible organizations of <u>all sizes</u> can participate while maintaining strong and consistent consumer protections.

FDATA respectfully offers the following comments on accreditation and other key implementation issues, and stands ready to continue to provide the Department of Finance ("the

Department") and the Bank of Canada with additional perspectives, including pertaining to the recommendations set out below.

I. Accreditation & Additional Sponsored Fintech Model Proposal

FDATA commends the Department for developing an accreditation framework that recognizes the differing regulatory obligations already borne by various types of market participants. The proposed regulations establish four accreditation pathways: a non-streamlined pathway, a streamlined pathway for entities registered under the Retail Payment Activities Act ("RPAA"), a pathway for federal and provincial financial institutions, and a pathway for accredited third-party service providers ("ATSPs"). This structure appropriately seeks to avoid unnecessary duplication of existing regulatory oversight for entities registered under the RPAA and federal and provincial financial institutions.

However, while the proposed framework successfully reduces duplication for already-regulated entities, it also has the unintended consequence of creating disproportionate barriers for the very firms that Canada's consumer-driven banking framework is intended to encourage. Small fintechs, startups, and merchants that do not hold RPAA registration would be required to navigate the full non-streamlined accreditation process even if they present comparatively limited risk. Historically, these small firms and startups tend to be the most innovative participants in open banking ecosystems around the world, despite operating with limited financial and administrative resources.

Simply put, if accreditation costs are too burdensome for small firms and startups, Canada's framework risks encouraging market exit – not market entry – thereby reducing the competition and innovation that the CDBA was designed to foster. This risk reinforces the case for a dual accreditation and operating model – one that allows providers to choose between full independent accreditation and a sponsored pathway – rather than forcing all participants into a single, restrictive operating model. More fundamentally, the current product development and monetization restrictions attached to each accreditation pathway independently constrain providers' ability to build and commercialize innovative, data-driven solutions. The result is a framework that risks entrenching incumbent banks' existing advantages, rather than enabling new entrants to develop differentiated products that expand consumer choice and deliver better financial outcomes.

Consistent with FDATA's previous submissions to the Department and the Bank of Canada, we believe the proposed accreditation framework inverts the appropriate allocation of regulatory burden, contrary to the intent of the CDBA. Rather than requiring every small fintech to independently satisfy comprehensive accreditation requirements, FDATA believes that aggregators serving as the central nodes within the ecosystem should have the opportunity to bear the more substantial accreditation obligations on behalf of the smaller firms that connect exclusively through aggregators' infrastructure.

To address this issue, FDATA has previously proposed a Sponsored Fintech Model, which would establish an additional, optional pathway for participation within Canada's CDB framework.[1] Under this approach, accredited aggregators have the option to assume responsibility for satisfying comprehensive regulatory requirements while sponsoring eligible participating entities that connect exclusively through their accredited infrastructure. Sponsored fintechs would continue to remain subject to applicable legal obligations under the CDBA and other relevant statutes, but would benefit from proportionate regulatory treatment that reflects their reduced operational footprint and reliance on accredited infrastructure.

FDATA believes such a structure would be consistent with the principle of proportionate regulation, under which regulatory obligations follow operational responsibility and ecosystem risk. Entities responsible for connectivity, authentication, consent management, and the secure operation of shared infrastructure should have the opportunity to bear greater regulatory obligations than application providers operating through that infrastructure.

Importantly, the Sponsored Fintech Model is not intended to replace the existing third-party service provider accreditation requirements. Rather, it would supplement the existing framework by creating an additional participation option for smaller market participants that may otherwise find accreditation prohibitively expensive or administratively burdensome. This approach would preserve robust consumer protections while reducing unnecessary barriers to market entry and encouraging continued innovation and competition.

FDATA continues to believe that the Department possesses sufficient authority under both the CDBA and the Data Mobility Amendment to Personal Information Protection and Electronic Documents Act ("PIPEDA") to establish such a model through regulation. Similar concepts have been successfully incorporated into open banking and financial services frameworks in other jurisdictions, demonstrating that proportionate accreditation can coexist with rigorous oversight and consumer protection. By lowering unnecessary barriers to participation while preserving robust oversight, this approach would encourage continued investment, accelerate product development, expand consumer choice, and strengthen the long-term competitiveness of Canada's CDB ecosystem. This approach would also significantly reduce the risk of mass market exit that Canada might face if it moves forward without such an approach.

II. Specific Feedback on Accreditation

Beyond FDATA's broader recommendation that the Department establish a Sponsored Fintech Model, FDATA offers several additional recommendations and requests for clarification regarding the proposed accreditation framework. Collectively, these recommendations are intended to improve regulatory certainty, promote proportionate oversight, and facilitate efficient

[1] *See* FDATA's Sponsored Fintech Participation Under the Consumer-Driven Banking Act, A Framework for Aggregator-Sponsored Accreditation, https://mcusercontent.com/d62b8c1570b4b45285fbb8f4b/files/ded9edfd-93a8-9754-ad71-c6cf97672f9d/FDATA_Sponsored_Fintech_Model_Proposal_69_.pdf, June 8, 2026.

implementation while preserving the high standards for consumer protection and operational resilience established under the CDBA.

Accreditation Sequencing

Regardless of the accreditation framework ultimately adopted, FDATA strongly encourages the Department and the Bank of Canada to publish the final accreditation criteria, detailed application guidance, and the designation of the technical standards body well in advance of implementation of the Act. Specifically, FDATA recommends that these foundational elements be finalized at least *nine months before accreditation applications are accepted*.

Providing market participants with sufficient implementation time will enable organizations of every size to prepare in parallel, make necessary investments in compliance and technology, and submit complete, high-quality applications once the accreditation process begins. Early publication of accreditation criteria will also reduce uncertainty throughout the market, improve the quality of applications received by the Bank of Canada, and accelerate the realization of the consumer benefits envisioned by the CDBA. Establishing regulatory certainty before implementation is one of the most effective ways to promote both timely market participation and long-term operational stability.

Streamlined accreditation for PSPs

FDATA strongly supports the proposed streamlined accreditation pathway for payment service providers ("PSPs") registered under the RPAA. This approach appropriately recognizes that RPAA-registered entities are already subject to comprehensive oversight by the Bank of Canada, including requirements related to operational risk management, safeguarding of end-user funds, incident reporting, and other prudential obligations. Avoiding duplicative regulatory reviews for these entities reflects sound regulatory design and allows both regulators and market participants to focus resources where they are most needed.

Several FDATA members are registered under the RPAA, and the proposed alignment between the RPAA and the CDBA accreditation framework will significantly reduce unnecessary administrative burden while maintaining robust consumer protections. FDATA encourages the Department to preserve this streamlined approach in the final regulations, as it appropriately recognizes existing regulatory supervision without compromising the integrity of Canada's CDB framework.

International open finance framework compliance

The proposed accreditation requirements for third-party service providers require applicants to disclose whether they are, or have sought to become, accredited or registered under CDB or open finance frameworks in other jurisdictions. While FDATA supports the inclusion of this information as part of the application process, the proposed regulations do not explain how it will be considered when evaluating an applicant's suitability for accreditation.

FDATA believes that an applicant's demonstrated compliance with comparable regulatory frameworks in other jurisdictions should be recognized as a meaningful indicator of organizational maturity, operational capability, and good character. Several FDATA members currently participate in and are regulated under established open banking ecosystems around the world and have successfully demonstrated compliance with rigorous regulatory requirements governing security, operational resilience, consumer protection, and data governance. These experiences provide valuable evidence that an applicant possesses the expertise and governance necessary to participate responsibly in Canada's CDB framework.

Recognition of good standing under comparable foreign regimes would be particularly valuable during the initial implementation of the CDBA, when the Bank of Canada will be reviewing a significant number of first-time accreditation applications. While foreign accreditation should not replace Canada's own review process, it should be considered as relevant evidence supporting an applicant's ability to satisfy the objectives of the CDBA. Incorporating this consideration would both improve regulatory efficiency and encourage participation by experienced market participants that have already demonstrated responsible operation within mature open finance ecosystems.

National Security Reviews

Several FDATA members serving Canadian consumers are headquartered outside of Canada but maintain substantial operations within the Canadian market. As a result, a number of these organizations will be subject to the Minister of Finance's national security review process as part of the proposed accreditation framework. FDATA recognizes and supports the importance of protecting Canada's national security interests and appreciates the inclusion of appropriate review authorities within the accreditation process. However, the proposed regulations provide limited guidance regarding the circumstances under which an application may be subject to the longer review timelines associated with national security assessments. Greater transparency regarding the factors that may trigger an extended review would provide applicants with greater certainty, facilitate implementation planning, and reduce unnecessary delays.

FDATA also believes that an applicant's demonstrated compliance with comparable regulatory frameworks in trusted foreign jurisdictions should be considered as part of this assessment. Organizations that are already subject to robust financial services regulation, maintain strong operational and cybersecurity controls, and have established records of compliance should generally not be expected to undergo extended review timelines absent specific national security concerns. FDATA encourages a risk-based approach that would allow regulatory resources to be directed toward applications that present genuinely novel or heightened risks while enabling experienced, well-regulated organizations to begin participating in Canada's consumer-driven banking framework without unnecessary delay.

III. Request for Clarity on Key Terms

FDATA believes the proposed regulations establish a strong foundation for implementing Canada's consumer-driven banking framework. However, several key terms would benefit from additional clarification to ensure consistent interpretation and implementation across the entire ecosystem. Providing greater certainty in these areas will reduce the likelihood of inconsistent application, minimize unnecessary disputes between market participants, and promote a more predictable accreditation and operational framework.

"Place of business in Canada"

The proposed regulations require participating entities to declare that they maintain a place of business in Canada but do not define what constitutes a "place of business" for the purposes of accreditation. Nor do the proposed regulations specify when such a presence must be established for entities that currently provide services to Canadian consumers without maintaining a physical Canadian office.

FDATA respectfully requests that the Department provide additional guidance regarding both the meaning of this requirement and the timeline for compliance. Clarifying whether a place of business requires a physical office, Canadian employees, or another form of legal presence would provide prospective participants with greater certainty as they prepare for accreditation.

In addition, FDATA recommends that the Department consider providing a reasonable transition period for otherwise qualified entities that currently operate within the Canadian market but do not yet maintain a formal place of business in Canada. Such a transition period would allow organizations sufficient time to establish an appropriate Canadian presence without unnecessarily delaying their participation in the CDB framework. This approach would preserve the policy objective underlying the requirement while avoiding unnecessary market exit.

"Insurance or Comparable Guarantees"

The proposed regulations require accredited entities to maintain "insurance or comparable guarantees" as a condition of accreditation but provide little guidance regarding what constitutes an acceptable guarantee, how adequacy will be assessed, or how required coverage should vary depending upon the nature and scale of a participating entity's activities.

FDATA supports the objective of ensuring that accredited participants possess adequate financial resources to protect consumers and support confidence in the ecosystem. However, greater clarity regarding these requirements would improve predictability for prospective applicants and facilitate more efficient accreditation decisions.

Accordingly, FDATA recommends that the Department clarify what forms of insurance or financial guarantees will satisfy this requirement, identify the criteria that will be used to assess adequacy, and explain how coverage expectations will be calibrated based on an entity's size, business model, and operational risk profile. A proportionate, risk-based approach would ensure that consumer protections remain robust while avoiding unnecessarily burdensome requirements for smaller market participants whose activities present comparatively limited risk.

"Derived Data"

FDATA supports the CDBA's exclusion of "derived data." However, the Department's statutory definition, which refers to data that has been enhanced to "significantly increase its usefulness or commercial value," introduces uncertainty as the term "significantly" is inherently subjective and is not further defined in either the CDBA or the proposed regulations.

Without additional guidance, participating entities may reach inconsistent conclusions regarding whether particular information constitutes in-scope consumer data or excluded derived data. This uncertainty creates the risk that ordinary account information could be characterized as derived data in order to withhold information from consumers or impose charges for access. Such outcomes would undermine the data portability rights established by Parliament and create unnecessary disputes throughout the ecosystem.

FDATA therefore encourages the Department to provide additional clarity regarding what constitutes a "significant" enhancement. This could be accomplished through illustrative examples in the final regulations, accompanying guidance issued by the Bank of Canada, or the development of an objective materiality test that distinguishes ordinary processing or formatting from genuinely value-added information. Establishing a clear threshold would promote consistent implementation across market participants while preserving Parliament's intent that consumers retain meaningful control over their financial information. Greater certainty regarding derived data will also encourage investment in high-value use cases, including fraud prevention, affordability analysis, categorization and normalization of transactions, behavioral analytics, and AI-enabled risk models that depend upon organizations' ability to responsibly transform consumer-permissioned data into new intelligence while remaining fully aligned with consumer consent.

"Significant Change"

Section 44 of the proposed regulations requires consumers to renew their consent following a "significant change," yet the regulations do not define what types of changes would trigger this requirement. While FDATA supports requiring renewed consent when material aspects of a consumer's authorization change, additional guidance is necessary to ensure that this obligation is interpreted consistently across participating entities. FDATA recommends that the Department clarify the types of changes that should be considered "significant" for the purposes of consent renewal, including whether the term is intended to encompass changes to the scope of data shared, the purpose for which data is used, participating entities, security practices, or other material aspects of the consumer relationship.

Conversely, routine operational or administrative changes that do not affect a consumer's substantive authorization should not require renewed consent. Providing illustrative examples or objective criteria for what constitutes a "significant change" would promote consistency throughout the ecosystem, reduce unnecessary consent fatigue for consumers, and ensure that consent renewals remain focused on circumstances in which consumers genuinely need to reconsider or reaffirm their authorization.

This clarity is particularly important for ongoing services that consumers expect to operate seamlessly, including recurring payment arrangements, revolving lines of credit, every-day financial management tools, etc. If consumers are required to reauthorize consent following changes that are administrative rather than substantive, they may inadvertently interrupt authorized services on which they rely or forget to renew consent altogether, potentially resulting in missed or delayed payments, overdrafts, or loss of credit availability despite their original intent to maintain the service. A clear, risk-based interpretation of "significant change" will help preserve meaningful consumer control while avoiding unnecessary disruption to established financial relationships.

IV. Data Scope

FDATA strongly supports the proposed scope of data included within the framework and believes it appropriately reflects both the intent and the requirements of the CDBA. The proposed regulations strike an appropriate balance between ensuring that consumers have meaningful access to the financial information necessary to exercise their data mobility rights while maintaining reasonable limitations consistent with the statutory framework.

FDATA particularly commends the Department for including product data within the scope of shareable information. Product information is essential to many of the most pro-competitive use cases enabled by consumer-driven banking, including comparison shopping, financial product recommendations, and the development of tools that help consumers and SMEs identify products that better meet their financial needs. Consumers cannot effectively compare products or switch providers if accurate and current product information is unavailable. Including product data alongside consumer financial information will therefore enhance competition and encourage financial institutions to compete on price, quality, and innovation.

FDATA believes the proposed scope establishes an appropriate foundation for Canada's CDB ecosystem and encourages the Department to retain these provisions in the final regulations.

V. Uses of Data

FDATA supports the CDBA's underlying principle that consumers should retain meaningful control over how their financial data is used and that participating entities should not use consumer data in ways that consumers neither authorize nor reasonably expect. Clear limitations on the use of consumer-permissioned data are fundamental to maintaining public confidence in the CDB framework and ensuring that consumers remain willing to exercise their data rights.

At the same time, the CDBA's objectives extend beyond consumer protection alone. Parliament also established the framework to encourage greater competition and innovation throughout Canada's financial services market. As such, restrictions on data use should be implemented in a manner that protects consumers while facilitating competitive neutrality between incumbent financial institutions and new market entrants and fostering innovation in financial products and services for the benefit of Canadian consumers and small businesses.

FDATA appreciates the additional clarity provided by the proposed regulations regarding permissible secondary uses of consumer data that are consistent with PIPEDA. However, the final regulations would benefit from further clarification confirming that consumer-permissioned data may be used to improve existing products and services, strengthen fraud detection capabilities, enhance cybersecurity, and develop more effective risk management models. FDATA also encourages the Department to clarify that, where consistent with consumer consent and applicable privacy law, consumer-permissioned data may be used for research, testing, and the development of new products and services. Allowing responsible product development is fully consistent with the CDBA's objective of fostering innovation while maintaining appropriate consumer protections. Importantly, these activities are routinely undertaken by incumbent financial institutions using the customer information already in their possession.

Providing this clarification would: (1) create market parity and enable participating entities to better compete with incumbents on equal terms while continuing to invest in product improvements and fraud prevention measures that directly benefit consumers; and (2) support the development of a more secure ecosystem by enabling participating entities to identify emerging fraud patterns and strengthen risk models without creating uncertainty regarding permissible internal uses of consumer-permissioned data.

VI. Consent and Authentication

FDATA strongly supports the proposed allocation of responsibilities between data requestors and data providers. Under the proposed framework, the data requestor is responsible for obtaining and managing the consumer's consent, while the data provider remains responsible for authenticating the consumer before data is shared. FDATA believes this allocation appropriately assigns responsibilities to the parties best positioned to perform them and reflects sound operational and regulatory principles. This approach also enables financial institutions to continue satisfying their existing legal and security obligations while ensuring that consumers maintain a direct relationship with the entity requesting access to their information. Clearly delineating these responsibilities will improve accountability across the ecosystem and reduce uncertainty regarding the respective obligations of participating entities.

While FDATA supports this overall framework, we believe that technical implementation will be equally important to ensuring a positive consumer experience. In particular, FDATA encourages the designated technical standards body to develop standardized user experience requirements governing authentication and redirection flows. Consumers should encounter a consistent, familiar authentication experience regardless of the financial institution involved, or whether they are digitally native or fluent. Standardization will strengthen consumer confidence, reduce confusion, and reinforce trust in CDB as Canadians begin exercising their data mobility and portability rights.

FDATA notes that unnecessary authentication friction could undermine the success of Canada's CDB framework. Experience in other jurisdictions (such as the European Union) has demonstrated that excessive or inconsistent authentication requirements can materially reduce successful consumer authorizations, even where consumers have clearly expressed their intent to share their data. Accordingly, FDATA recommends that the designated technical standards body establish a standardized, minimum set of authentication screens and user interactions that all participating data providers must follow, and provide approved authentication pathways for Canadians who do not have, or choose not to use, online banking credentials. Such standards would preserve strong authentication while preventing unnecessary obstacles from being introduced into the consumer journey.

FDATA further encourages the Department to ensure that any requirements regarding consent do not frustrate consumers' ability to choose products and services most beneficial to them. For example, the proposal should allow consumers to expressly consent to periods longer than 12 months. And the Department should consider opportunities to streamline the consent renewal process. Consent renewal should continue to provide consumers with meaningful control over their data while avoiding unnecessary friction that may discourage continued use of CDB services. This consideration will be particularly important for emerging use cases such as pay-by-bank, where excessive consent requirements could place consumer-driven payment solutions at a competitive disadvantage relative to established card-based payment systems.

Consistent with the approach successfully adopted in the United Kingdom, FDATA recommends that the final regulations permit consent and consent renewal to be managed by the data requestor or its ATSP. This model has proven effective in reducing unnecessary consumer friction while preserving consumer control over data sharing decisions, providing a more seamless user experience without diminishing transparency or accountability.

Finally, FDATA recommends that the final regulations clarify that, where an accredited entity participates in more than one accredited capacity with respect to a single consumer relationship, a single, clear consent flow should be sufficient for that connection. Consumers should not be required to complete multiple consent processes for what is, in substance, a single authorized activity. Similarly, the Department should confirm that, with the consumer's informed and explicit consent, a single consumer connection may appropriately support two participating entities where doing so reflects the consumer's intended use of the services. For example, a consumer may use a financial service provided by a participating entity to view and manage their financial accounts and, within that same experience, elect to receive a complementary service provided by a second participating entity. Where the consumer is clearly informed of both entities, the data each will receive, and the purposes for which the data will be used, the consumer should be able to authorize both services through a single connection and consent flow. Consequently, data providers' technical implementations should be able to accommodate more than one authorized entity. These clarifications would simplify implementation, reduce unnecessary consent fatigue, and further the CDBA's objective of creating a consumer-friendly and competitive open banking ecosystem.

VII. Data Deletion

FDATA supports the proposed clarification that participating entities are not required to delete data that has been irreversibly or permanently modified. This clarification appropriately recognizes that certain information may be transformed through aggregation, anonymization, or other permanent modifications such that it can no longer reasonably be considered consumer data subject to deletion requirements. Providing this certainty promotes consistency across the ecosystem while allowing participating entities to retain information necessary for legitimate business, operational, and legal purposes. FDATA believes the proposed approach appropriately balances consumers' rights to control their financial information with the practical realities of operating secure and innovative financial services.

FDATA also recommends clarifying that data need not be deleted where its retention remains reasonably necessary for an ongoing permitted use that is consistent with the consumer's consent and the CDBA. This includes circumstances where historical data is required to validate, monitor, maintain, or improve fraud detection systems, cybersecurity capabilities, credit and risk models, or other operational models that continue to rely on historical training and performance data. Such a clarification would align consumer protections with practical operational requirements while avoiding unnecessary disruption to legitimate, consented activities and important services.

VIII. No Charge for Data Sharing

FDATA strongly supports the CDBA's prohibition on charging for consumer-permissioned data sharing. This principle reflects the fundamental premise that consumers and SMEs own their own financial information and should not be required to pay to exercise their statutory right to direct that information to a participating entity of their choosing. Ensuring that access to consumer-permissioned data remains free is essential to promoting competition, reducing barriers to switching financial service providers, and encouraging innovation throughout Canada's financial services ecosystem.

While FDATA supports this prohibition, the proposed regulations would benefit from additional clarification regarding its application to ATSPs, particularly where those entities are owned or controlled by one or more mandated data providers. Without greater clarity, uncertainty remains regarding whether a data provider could indirectly impose charges through an affiliated service provider despite being prohibited from doing so directly.

FDATA believes that the role performed by an ATSP should determine whether charging is permissible. Where an ATSP provides "data out" services on behalf of a data provider, it is effectively acting as an extension of that data provider. In those circumstances, the ATSP should be prohibited from charging the data requestor for access to consumer-permissioned data under the CDBA, just as the data provider itself would be prohibited from doing so.

Conversely, where an ATSP provides "data in" services on behalf of a data requestor, it is acting as a service provider to that requestor rather than to the data provider. In that circumstance, the ATSP should remain free to charge its client in accordance with ordinary commercial arrangements. Nothing in the CDBA should prevent private contractual relationships between a data requestor and its chosen technology provider.

FDATA recognizes that certain ATSPs may perform both data-out and data-in functions. Nevertheless, the same principle should continue to apply based upon the role being performed. Under no circumstances should an ATSP providing data-out services to data providers be permitted to leverage that position to obtain market share through preferential access arrangements before subsequently imposing charges on competing data requestors. Such an outcome would be inconsistent with the objectives of the CDBA and would be particularly concerning where the ATSP is owned or controlled by the very institutions required to share consumer data.

FDATA additionally recommends that the final regulations expressly state that the prohibition on charging for data access extends not only to the sharing of in-scope consumer data, but also to authenticating consumers on behalf of a data provider. Rather than leaving this principle to implication, the regulations should clearly provide that no data provider, either directly or through any third-party service provider acting on its behalf, may impose a charge on either a consumer or a data requestor for the sharing of in-scope data or for any activity associated with granting, maintaining, renewing, or withdrawing consent. Such express language would eliminate ambiguity and prevent the development of business models that undermine Parliament's intent.

This clarification is particularly important where an ATSP is owned or controlled by one or more mandated data providers. A data provider should not be permitted to accomplish indirectly or through a jointly owned intermediary what it is expressly prohibited from doing directly. Allowing such entities to impose access or consent-related charges would create an uneven competitive landscape and weaken one of the CDBA's core consumer protections.

FDATA also encourages the Department to clarify that consumer-permissioned access to data should not be characterized as "write" access merely because the data may be used in connection with a downstream payment or other transaction. FDATA's understanding is that "write" access should be limited to circumstances in which a third party takes an action on behalf of the consumer with respect to the account, such as initiating a payment on behalf of the consumer from the account. Correspondingly, any payment mechanism that does not require the consumer to affirmatively initiate the transaction (such as an EFT debit) should not be considered write access.

Absent clear guidance distinguishing data access from payment initiation, data providers could classify read activity as a write function, potentially restricting access or imposing charges that frustrate the CDBA's objectives.

The framework proposed by FDATA would align Canada's consumer-driven banking regime with open finance frameworks internationally, some of which have adopted similar approaches to prevent anticompetitive outcomes while preserving appropriate commercial relationships between technology providers and their clients.

IX. Duty to Share Exemptions

FDATA recognizes that the circumstances under which a data provider may refuse to share consumer-permissioned data are among the most consequential provisions within the proposed framework. Properly calibrated exceptions protect consumers, preserve the security and integrity of the financial system, and maintain confidence in the ecosystem. At the same time, overly broad or inconsistently applied exceptions have the potential to undermine competition by allowing data providers to deny legitimate requests for data access. FDATA therefore commends the Department's efforts to narrowly tailor the exceptions contained in section 35(1) of the proposed regulations.

Overall, FDATA believes the proposed exceptions appropriately reflect legitimate risk management considerations. However, the Department should consider supplementing the final regulations with illustrative guidance describing the circumstances in which each exception may appropriately be invoked. Providing practical examples would promote greater consistency across participating entities and reduce the likelihood of divergent interpretations that could create unnecessary disputes.

FDATA also strongly supports the proposed requirement that data providers notify both the data requestor and the Bank of Canada whenever a request for data sharing is denied. Transparency surrounding refusals is critical to ensuring accountability throughout the ecosystem and allowing regulators to identify patterns that may indicate inappropriate or inconsistent application of the exceptions.

FDATA further recommends that this notification obligation expressly apply where a request is denied on the basis that the requested information constitutes excluded derived data. Because the distinction between covered data and derived data may involve the exercise of judgment, transparency regarding these decisions is essential. Requiring notification would ensure that any inappropriate characterization of covered consumer data as derived data is visible to both the requesting entity and the Bank of Canada, thereby discouraging misuse of the derived-data exclusion and supporting Parliament's intent to establish meaningful consumer data portability rights.

X. Service Levels

FDATA generally supports the proposed service level requirements and believes they establish an appropriate baseline for reliable participation in Canada's CDB ecosystem. Although these requirements are technical in nature, experience from other jurisdictions has demonstrated that service levels can become a significant nexus of anticompetitive behavior if not accompanied by clear and enforceable non-discrimination obligations. Reliable, timely, and consistent API performance is essential to ensuring that consumers receive the benefits promised by consumer-driven banking.

FDATA is particularly supportive of proposed subsection 36(1)(c), which establishes a non-discrimination obligation with respect to traffic management. This provision appropriately recognizes that participating entities should not be permitted to disadvantage certain requestors through differential treatment of API traffic or other technical means.

For the avoidance of doubt, however, FDATA recommends that the final regulations expressly clarify that this obligation extends equally to ATSPs providing data-out services on behalf of data providers. Such clarification would ensure that non-discrimination principles apply consistently throughout the ecosystem, regardless of which entity is operating the technical infrastructure.

FDATA also supports the proposed requirements relating to 99.5 percent API uptime, generally accepted response times, and the availability of twenty-four months of transaction history. Collectively, these requirements establish an important foundation for ensuring that consumer-driven banking services are dependable, competitive, and capable of supporting a wide range of innovative financial products. To ensure that data providers do not hamstring or disadvantage consumer-permissioned access, FDATA further recommends that performance and availability obligations are benchmarked against data providers' own first-party digital channels. The Bank of Canada, as the senior governing body, may operate (or designate an operator for) a conformance testing program against which endpoint compliance, uptime, and response-time obligations can be objectively and consistently verified.

XI. Liability

FDATA applauds the proposed liability framework, which represents meaningful progress toward operationalizing the widely supported principle that liability should follow the data. While this concept has long enjoyed broad support in principle, market participants have often struggled to translate it into a practical allocation of responsibilities. The proposed regulations make important progress by clearly distinguishing the respective obligations of data requestors and data providers. Under the proposed framework, data requestors are responsible for obtaining consumer consent and appropriately receiving consumer data, while data providers remain responsible for authenticating consumers and securely providing the requested information.

FDATA believes this allocation appropriately reflects the functions performed by each participant, creates stronger accountability throughout the ecosystem, and provides consumers with greater certainty regarding which entity bears responsibility when issues arise.

At the same time, FDATA notes that additional clarification may be appropriate in circumstances where actions by both the data provider and the data requestor contribute to a consumer loss. While the combination of the proposed liability allocation and the requirement that accredited entities maintain insurance or comparable guarantees should address the vast majority of circumstances, further guidance regarding shared responsibility scenarios would promote greater certainty and reduce the potential for disputes between participating entities.

XII. Screen Scraping

FDATA supports the long-term objective of eliminating screen scraping and replacing credential-based access with more reliable, standardized API connectivity. APIs provide significant improvements in reliability, transparency, and consumer control, and are essential to realizing the full benefits of consumer-driven banking. FDATA welcomes the Department's commitment to transitioning Canada's financial ecosystem toward API-based data sharing and stands ready to continue working with the Department and the Bank of Canada throughout that transition.

FDATA emphasizes that the success of this transition depends entirely upon the availability of high-quality, dependable, and consistently functioning APIs. Today, many Canadian consumers experience reliability limitations and degradation associated with credential-based data access that can be meaningfully resolved through high-quality, consistent connectivity that cannot be limited or degraded unilaterally by financial institutions. Without this, consumers may find themselves unable to use the services of their choosing. Accordingly, FDATA urges the Department to require data providers to make compliant APIs available on an expedited timeline so that consumers can begin realizing the benefits envisioned by the CDBA.

Finally, FDATA believes it is critical that any prohibition on screen scraping not take effect until participating data providers have demonstrated that their live API connections are robust, reliable, and consistently available over a sustained period of time, and that companies have time and ability to migrate users to APIs. Consumers should never experience a reduction in their ability to exercise their data mobility rights as a consequence of the transition to APIs, and need time to adapt. Delaying the prohibition until API performance has been proven in practice will provide an orderly transition, preserve continuity of service, and ensure that the implementation of consumer-driven banking enhances, rather than diminishes, consumer choice and access.

XIII. Conclusion

FDATA appreciates the Department's continued leadership in implementing the CDBA and developing a CDB framework that has the potential to become a global model for secure, competitive, and consumer-centric financial data sharing. The proposed regulations represent significant progress toward operationalizing Parliament's vision and establish many of the core elements necessary for a successful ecosystem.

As described throughout this submission, FDATA respectfully encourages the Department to consider several targeted refinements before finalizing the regulations. In particular, FDATA recommends that the Department:

- Establish an optional Sponsored Fintech Model to provide a proportionate pathway for smaller fintechs to participate in the ecosystem while maintaining robust consumer protections;
- Ensure that accreditation obligations remain proportionate to operational responsibility by recognizing the central role often played by aggregators;
- Publish final accreditation criteria, Bank of Canada application guidance, and technical standards well in advance of implementation to provide regulatory certainty and facilitate timely participation;
- Clarify key accreditation requirements and defined terms, including "place of business in Canada," "insurance or comparable guarantees," "derived data," and "significant change";
- Preserve the proposed scope of covered data, including product data, while providing additional clarity regarding permissible internal uses of consumer-permissioned data for product improvement, fraud prevention, and risk management;
- Clarify that consumer-permissioned data may, where appropriately consented to, be used for research, product development, fraud prevention, cybersecurity, and ongoing model validation;
- Maintain the proposed allocation of responsibilities between data requestors and data providers while reducing unnecessary authentication and consent friction through standardized technical requirements and streamlined consent management;
- Clarify that no participating entity, including affiliated ATSPs acting on behalf of data providers, may impose charges for sharing in-scope data or for obtaining, renewing, or withdrawing consumer consent;
- Provide additional guidance regarding the duty-to-share exceptions, including transparency requirements when requests are denied on the basis of the derived-data exclusion;
- Preserve strong service level requirements and confirm that non-discrimination obligations apply consistently across all entities operating technical infrastructure within the ecosystem;
- Continue refining the proposed liability framework by providing additional guidance regarding circumstances involving shared responsibility between participating entities; and
- Ensure that any prohibition on screen scraping takes effect only after compliant APIs have demonstrated sustained reliability, performance, and availability.

Taken together, these recommendations are intended to strengthen implementation of the CDBA while preserving its core objectives of promoting competition, innovation, consumer choice, and financial stability. FDATA believes that proportionate regulation, clear operational rules, and consistent technical standards will encourage broad market participation while maintaining the high levels of security and consumer protection that Canadians rightly expect.

FDATA also believes that the consumer-driven banking framework should be viewed not as an endpoint, but as foundational digital infrastructure for a broader open data ecosystem upon which the future of financial innovation will be built. As secure access to consumer data becomes standardized, competitive differentiation will increasingly come from the intelligence, services, and consumer outcomes built on top of that data. The long-term success of the CDBA will therefore be measured not simply by how effectively it enables the movement of financial information, but by how effectively it supports innovation, strengthens fraud prevention, promotes financial inclusion, expands consumer choice, and enables Canadians to make better financial decisions.

FDATA appreciates the opportunity to provide these comments and would welcome the opportunity to discuss any of the recommendations contained in this submission. We remain committed to working collaboratively with the Department, the Bank of Canada, and all stakeholders to support the successful implementation of Canada's consumer-driven banking framework.

Sincerely,

Steven Boms
Executive Director
FDATA