Fintechs Canada

Kïrsten Fraser
Director, Financial Services Innovation
Financial Services Division
Financial Sector Policy Branch
Department of Finance Canada
90 Elgin Street
Ottawa, Ontario K1A 0G5

August 26, 2026

[Via email]

Fintechs Canada extends its thanks to the Department of Finance Canada for the opportunity to respond to the consultation on the proposed Consumer-Driven Banking Regulations published in Canada Gazette Part I on July 26, 2026.

Fintechs Canada is the unified voice for the most innovative financial technology companies. Serving millions of Canadians daily, our more than 50 members include market-leading Canadian fintechs, fintech-friendly financial institutions, technology companies that power the credit union space, and global fintech companies. Our mission is to make Canada's financial sector more competitive and innovative while strengthening its stability and security.

We congratulate the federal government for advancing these and other important pro-competition reforms and welcome the publication of the proposed Regulations for Canada's Consumer-Driven Banking Framework. It will be critical that the regulatory framework provides clarity for participating entities without imposing undue rigidity that stifles fintech innovation. Through achieving this balance, the framework will support the government's objectives of increasing competition and consumer choice in the financial sector.

Canada's vision of success for consumer-driven banking should be regarded as a framework that is widely trusted and adopted by Canadians, enabling them to access an expanded range of financial services, giving them greater control over their data and agency over their finances, and access to more affordable financial

products. For SMEs, this includes greater access to capital. That adoption, in turn, will drive growth, productivity and innovation across the economy.

Fintechs Canada encourages the Bank of Canada and the Department of Finance to coordinate with other government departments and regulators at the federal and provincial levels to ensure that the consumer-driven banking framework takes into account the existing and emerging regulatory frameworks, including those overseeing payments, privacy and artificial intelligence, promoting alignment and reducing friction. This includes working with Payments Canada to ensure alignment and coordination on rules and requirements between consumer-driven banking and participation in the Real-Time Rail (RTR).

Finally, we urge Finance Canada to move forward swiftly with CDB's write-access. Switching friction in Canada's financial services is driven by operational barriers, not price alone, and Canadian consumers will not realize the full value of consumer-driven banking until they can act on their data, not just view it. Payment initiation, account funding, and pre-authorized debits (PAD) migration are the operational capabilities that make switching practical and resolve that friction. Deferring these capabilities to Phase II without an accelerated timeline will delay the framework's competitive impact

The sections below provide recommendations for key provisions of the consumer-driven banking regulations, to ensure that the consumer-driven banking framework is proportionate, risk-based, and accessible for Canada's fintech ecosystem.

Accreditation

Fintechs Canada welcomes the segmentation of accreditation for different participating entities. That said, the accreditation process should be risk-based and proportionate to avoid creating a barrier to entry for smaller fintechs. This is particularly important to attract and enable the participation of emerging players, fostering competition, innovation, and the scalability of fintech businesses in Canada.

The draft Regulations organize accreditation around four pathways, generally defined by entity type, rather than by the specific activities an entity performs. In practice, many participating entities operate across more than one category.

> **Example**: An entity may be RPAA-registered and at the same time provide services to other financial institutions rather than directly to consumers, or it may perform activities that fall within both a participating entity's obligations and an ATPSP's scope.

The current structure does not clarify how such entities are to be classified, and whether accreditation requirements are intended to attach to the entity as a whole or to the discrete activities it carries out. Nor do the proposed Regulations address how accreditation would apply to an entity that qualifies under more than one pathway simultaneously.

It is not clear whether such an entity would be required to complete separate accreditation processes under each applicable pathway, with distinct timelines, disclosure requirements, and registry publication dates, or whether a consolidated accreditation approach reflecting the full scope of an entity's activities is contemplated. The framework should clarify how accreditation will apply where an entity falls within more than one category. It should specify whether a firm can submit a single consolidated application covering all relevant activities or whether separate applications and fees will be required for each category.

More broadly, this entity-based categorization does not appear to calibrate accreditation requirements to the size of an applicant, its risk profile, or existing industry relationships and partnerships already in place in the market. The framework's stated objectives include increasing competition and enabling a broader range of participants; **the current structure's relationship to those objectives, particularly for smaller entities engaged in a narrower or more specialized set of activities, is not addressed in the proposed Regulations**. For smaller fintechs with limited data sets and a lower risk profile, we recommend that the government sets out a “Baseline” security tier, which we discuss under Security Requirements, below.

We welcome the streamlined accreditation pathway for entities registered under the Retail Payments Activities Act (RPAA), which recognizes that many fintechs participating in the consumer-driven banking framework are already subject to similar application requirements under the RPAA. That said, the pathway does not appear to meaningfully reduce the regulatory burden in practice, as it still requires new frameworks specific to consumer-driven banking. For the streamlined RPAA accreditation pathway to be successful, its requirements should not create

duplicative burdens for participating entities. We encourage the Bank of Canada to consider a mutual recognition model, under which an RPAA-registered entity is deemed to have met baseline security requirements unless specific gaps are identified.

Fintechs Canada also welcomes the ATPSP pathway. That said, the distinction between the ATPSP pathway's comparatively lighter accreditation requirements and the requirements applicable to other pathways is not fully reconciled with the framework's entity-based structure. An entity performing some activities within and outside that scope may face uncertainty as to which requirements govern which parts of its business, and how disclosures are to be organized accordingly. The term "third-party service provider" should be clearly defined so that entities can determine whether they fall within this category and, where they do, understand the specific requirements and obligations that apply.

Additionally, the Third-Party Service Provider (TPSP) category is limited to three activities: consent management, authentication management, and movement of data. Fintechs that perform services of payment initiation, identity verification tied to AML, and write-access use cases do not fit within these categories. The TPSP accreditation route also does not take into account existing industry partnerships such as B2B2C models between fintechs and merchants that operate across economic sectors. The Regulations should either consider expanding the TPSP categories and/or provide a more flexible pathway for accreditation of participating entities that accurately reflects industry dynamics. In addition, the Regulations should explicitly address *whether and how* ATPSP functions can expand over time as industry use cases evolve, rather than requiring future consultations each time new functions emerge.

Finally, Fintechs Canada urges for additional clarity on the accreditation process itself, through either a guide or readiness checklist through the Bank of Canada, to help participating entities in preparation and resource allocation.

Recommendations:

1. The accreditation process should avoid duplicative requirements by leveraging information that registered PSPs have already provided to the Bank of Canada under the RPAA. We encourage the Bank of Canada to consider a mutual recognition model, under which an RPAA-registered entity

is deemed to have met baseline requirements (including on security) unless specific gaps are identified.

2. The final regulations or accompanying guidance should address how accreditation would apply to an entity that qualifies under more than one pathway simultaneously, including whether a consolidated accreditation process is available, rather than requiring separate applications under each applicable pathway.
3. Accreditation requirements should be risk-based and proportionate to prevent unnecessary barriers to entry for smaller and emerging fintechs. For fintechs with limited data sets and a lower risk profile, we recommend that the government sets out a "Baseline" for security safeguards.
4. The term "third-party service provider" should be clearly defined to assist entities determine whether they fall under this category.
5. Consider expanding the "third-party service provider" categories to better reflect existing industry partnerships. Moreover, the Regulations should also build in greater flexibility for the future, explicitly addressing whether and how ATPSP functions can expand over time as industry use cases evolve, rather than requiring future consultations each time new functions emerge.
6. The Bank of Canada should publish clear accreditation guidance, such as a readiness checklist or implementation guide, to help participating entities prepare and allocate resources effectively. Greater clarity on accreditation fees is also needed through a definition of total asset value, including how it should be calculated and assets in scope.

Promoting competition through enabling secure participation of sponsored fintechs

The draft Regulations offer four accreditation pathways; however, none provide genuinely proportionate access for small or scaling-up fintechs. The non-streamlined pathway applies a uniform accreditation and compliance burden regardless of entity size, data volume, or risk profile. While the ATPSP route offers a calibrated opportunity for certain service providers, it is not a viable alternative for small fintechs operating as data recipients, for fintechs engaged in provision of services outside the TPSP scope, nor those with intermediary structures such as gateway-to-multiple-merchant chains.

The current framework is further structured around B2C relationships, which leaves out fintechs operating in a B2B2C model: those contracting with merchants whose end consumers use the fintech's payment infrastructure for pay-ins and pay-outs. Because these fintechs are not themselves consumer-facing, they fall outside the framework's scope as drafted, even though they hold the transaction data, customer data, and fraud/risk information relevant to consumer-driven banking cases.

Other jurisdictions have addressed the above gaps through sponsored accreditation models, which allow smaller, unaccredited entities to access the framework under the liability umbrella of a fully accredited sponsor. These models have served as a mechanism to extend framework access without requiring every downstream entity to independently pursue accreditation. Adopting a similar approach early could allow Canada to avoid barriers to access and competition that have emerged early on in other jurisdictions.

Under a sponsorship model, an accredited entity can also absorb liability for its downstream partners or vendors by contract, rather than requiring each entity in the chain to independently seek accreditation. Provided a sponsored fintech remains liable to its sponsor, and the sponsor remains liable to the framework, systemic risk does not increase. What does increase is participation, optionality, and the ability for smaller players to enter the market, build compliance maturity, and eventually graduate to full accreditation. A sponsorship model would also accommodate the hub-and-spoke commercial relationships already common in the market, without requiring non-payment businesses and merchants to seek accreditation they would otherwise have no reason to pursue.

> **Example**: Merchants engaged in B2C service delivery that rely on a fintech for payment processing or data verification, for example, do not necessarily operate in the financial services space themselves, and therefore have little incentive to seek CDB accreditation. Under the current draft Regulations, each such merchant would need to obtain its own accreditation to enable open banking access as the consumer-facing entity. In practice, merchants such as gaming operators, remittance companies, and corporates that outsource their payments would have no interest in becoming accredited entities, precisely because they outsource payments compliance in the first place. The likely outcome is that these merchants would decline to participate, consumers would lose access to open banking benefits through

these channels, and activity shifts back to direct bank relationships, which would undermine the framework's competition objective.

A sponsorship model would address the above concerns and reflect how the industry actually works. Partnerships, white-label arrangements, and platform relationships are already the dominant commercial model for many fintechs; a sponsorship pathway would formalize and regulate those relationships rather than leave them unaddressed.

To ensure this model is successful in the next phase of consumer-driven banking, the Regulations should confirm that sponsored entities would not be structurally excluded from future write-access capabilities once introduced, and that eligibility for write access will be based on the sponsor's accreditation and liability coverage rather than requiring the sponsored entity to separately hold direct accreditation.

Finally, Fintechs Canada submits that the final Regulations, or accompanying guidance, define a clear process and criteria for a sponsored entity to transition to full accreditation over time.

Recommendations:

7. Establish a sponsorship model for fintechs as an accreditation pathway which would better facilitate the participation of smaller players and accommodate existing B2B2C merchant models, without increasing systemic risks.
    a. The Regulations should confirm that sponsored entities are not structurally excluded from future write-access capabilities once introduced, and that eligibility for write access will be based on the sponsor's accreditation and liability coverage rather than requiring the sponsored entity to separately hold direct accreditation.
8. The final Regulations, or accompanying guidance, should define a clear process and criteria for a sponsored entity to transition to full accreditation over time.

Data Scope

The proposed Regulations outline the categories of consumer-permissioned data that must be made available for sharing under Canada's consumer-driven banking framework. While certain in-scope data is specifically defined, other categories of

in-scope data remain vague, which might create uncertainty for participating entities.

A lack of clarity could lead to inconsistent interpretations across data providers, uneven implementation by data recipients, and uncertainty for consumers about what information they can expect to access or share.

Product Data

"Product data" is broadly defined, but it is not clear whether this category is intended to capture detailed product terms, fee structures, eligibility criteria, promotional conditions, credit insurance, or interest rate ranges versus Annual Percentage Rates. For product and transaction data, in-scope data should include, at a minimum, the following fields: transaction ID, account ID, transaction date, transaction status, amount, transaction description, credit/debit indicator, bank code, transaction currency, account balance, merchant name, Merchant Category Code and creditor address. We suggest requiring a minimum of two years of historical transaction data, or data back to the date the account was opened where the account has been open for less than two years. Moreover, consumers should be permitted to authorize sharing of their full retained history up to five years where available, to support risk models that expand credit access.

The draft Regulations address consumer profile, account, and product data, but do not explicitly address whether the full scope of data visible to a consumer through their own online banking interface is captured. This leaves a **potential gap between what consumers can currently see about their own accounts and products, and what participating entities are obligated to make available for sharing. Clarity is required to ensure that the data scope includes all that is visible to the consumer**, such as specific rates/fees versus a generic read of the product, as well as the technical specifications such as data standards and format to ensure expectations are met for data sharing and extraction.

> **Example**: under the “read-access” framework, the visibility of data on payment transactions remains critical. Participating entities should be able to read key data associated with a payment, such as the amount, type and recipient, rather than a merely generic text such as “payment.” This is important to avoid friction within the system, allow the development of consumer-facing products, and realizing the full framework potential.

More explicit definitions of “product data” will further assist with segmenting genuine product data that is available to the consumer versus commercially sensitive data. A definition of “commercially sensitive information” would prevent the forced disclosure of trade secrets under the guise of “product data” (e.g. exclude proprietary risk-scoring algorithms, internal pricing models, etc), striking a balance that promotes genuine competition.

Account Data

For Account Data, specifically account identifiers, in-scope data should include, at a minimum, the following fields: account ID, account status, account type (e.g. business, current, savings or credit card), party type (e.g. sole or joint), currency, full legal name of the account holder(s), address of the account holder(s), date of birth of the account holder(s), credit-line limit, and account opening date. Where an account is held jointly, the relevant party information should be provided for each account holder.

Finally, account-ownership verification and payee confirmation should contemplate uses of consented data, which would support RTR's verification expectations.

Derived Data

The draft Regulations do not provide a clear definition of derived data, nor is there specificity on where the boundary lies between data that must be shared under the framework and derived data that a participating entity may treat as proprietary. In particular, it should be confirmed whether outputs created using consumer-driven banking data, such as transaction categorization, affordability indicators, or credit-risk scores, fall in or outside the regulated data scope, and whether firms remain free to use and commercialize those outputs. This should be addressed in forthcoming regulatory guidance.

Scope and Rollout

Beyond the above definitional questions, the proposed Regulations indicate that the coming-into-force of account types will be staggered, beginning with deposit and payment accounts, followed by lending accounts, then registered accounts, and finally non-registered accounts. Fintechs Canada urges regulatory clarity on the exact phasing of this account rollout, such as a prescribed timeline in the final

Regulations, to ensure that the industry can prepare and to avoid further implementation delays. Similarly, clarity is needed on what is required in the first year regarding terms and conditions, investments and other scope items not common across current online banking interfaces.

> **Example**: Registered and non-registered investment accounts are currently scheduled to come into scope in close succession, with both effectively required within the same year of rollout. Investment account types tend to be more varied in structure than deposit, payment, or lending accounts, and are often serviced through multiple affiliates or subsidiaries. In addition, the industry data standards needed to support consistent implementation for these account types are either non-existent or under development, combined with uncertainty surrounding the designation of a technical standards-setting body. Given this combination of factors, further clarity on the implementation timeline for all accounts, including how readiness of the applicable data standards will be assessed and communicated, would help participating entities, and the affiliated entities that must be brought into the framework alongside them, plan and prepare accordingly.

Transparency throughout the rollout period, between the publication of final regulations and the launch of participant applications, will be paramount to minimizing disruption and maximizing value creation for the consumer.

Recommendations:

9. "Product data" should be further defined to avoid any potential confusion or uncertainty for participating entities. In-scope data should include, at a minimum, the following fields: Transaction ID, Account ID, transaction date, transaction status, amount, transaction description, credit/debit indicator, bank code, transaction currency, account balance, merchant name, Merchant Category Code and creditor address. A minimum of two years of historical transaction data, or data back to the date the account was opened where the account has been open for less than two years, should be required. Consumers should be permitted to authorize sharing of their full retained history up to five years where available to support risk models that expand credit access.
10. "Account data" should include Account ID, account status, account type, party type, currency, full legal name of the account holder(s), address of the

account holder(s), date of birth of the account holder(s), credit-line limit, and account opening date.

11. Clarify the definition of "derived data", including the segmentation of data that could be considered proprietary.
12. The Regulations should provide further clarity on the sequencing of the rollout of account types, through a prescribed timeline in the final Regulations, to help participating entities properly prepare.

National Security Safeguards

Fintechs Canada recommends that the national security review be transparent to ensure that prospective participating entities have visibility into the process and queuing system, such as review triggers. This would also help remove any uncertainty for participating entities and, in turn, support a well-functioning framework.

Regarding timelines, a maximum aggregate timeline would provide applicants with greater certainty.

Consideration should also be given to whether the timeline should differ for applicants that are already registered under the RPAA and have undergone a similar national security review as part of that process.

Recommendation:

13. The national security review must be transparent to ensure that prospective participating entities have visibility into the process. A maximum aggregate timeline would provide applicants with greater certainty.

Security Requirements

The proposed Regulations require that a breach of security safeguards involving consumer data be reported to the Bank of Canada as soon as feasible, with the reporting responsibility resting on the entity in control of the data at the time of the breach. In practice, many participating entities also registered under the Retail Payments Activities Act (RPAA), are subject to that framework's breach-reporting obligations. The proposed Regulations do not address how these two reporting regimes interact where a breach falls within the scope of both frameworks, including which entity is responsible for reporting and through which channel.

In addition, the requirement to report a breach of the security safeguards to the Bank of Canada "as soon as feasible" would benefit from a clearly defined **maximum reporting timeframe**. We would also welcome clarity on how this obligation will interact with breach notification requirements under PIPEDA, any successor federal privacy legislation and applicable provincial regimes, to avoid conflicting timelines or duplicative consumer notifications arising from the same incident.

There is also a perceived duplication between RPAA compliance obligations and open banking accreditation requirements, particularly around audit and security review. This overlap is expected to grow more complex once write access is introduced, potentially resulting in a multi-tier compliance structure rather than integration.

Relatedly, the proposed Regulations appear to create a gap between ATPSPs and other participating entities with respect to independent third-party confirmation of security safeguards. Practically, this apparent discrepancy could create friction as participating entities develop business arrangement contracts and implement internal compliance processes with ATPSPs whose security safeguards are confirmed under a different standard. The Regulations should provide clarity on the security requirements applicable to all participating entities, including how these requirements are intended to align across entities that may be contracting with one another under the framework.

To this end, further clarity is needed on how the section 37 safeguards apply to different types of participants. In particular, the framework should specify which obligations apply directly to each entity and how responsibility is allocated where activities are outsourced, to avoid both gaps and unnecessary duplication in security controls.

To ensure that all participating entities, regardless of size, meet a uniform level of protection, the Bank of Canada should issue a Consumer-Driven Banking Security Baseline. A baseline should mandate specific technical standards, such as FAPI 2.0 for connectivity, and measurable technical compliance metrics. The prescriptive bar should rise with risk and be calibrated by data volume.

The regulations should further confirm that existing penetration testing and incident-response exercises conducted under recognized frameworks such as ISO

27001 or SOC 2, or participation in sector-wide exercises, can satisfy security requirements, provided that their scope covers the data sharing systems. Ultimately, the framework should avoid requiring separate, duplicative testing exercises where the scope condition has already been met.

Given that evidence of compliance with the technical standard will be required as part of accreditation under section 3(1)(m), further clarity on implementation timelines would assist firms with planning. In particular, we would welcome information on when the technical standards body is expected to be designated, when the standard under section 125(1) is expected to be published, whether it will include API security or authentication requirements beyond those in section 37, and the implementation period that participating entities will be given to demonstrate compliance.

Recommendations:

14. Security requirements should be calibrated to the nature, scale, complexity, role, and data access of each participating entity, including whether the entity is a data provider, data recipient, or is outsourcing functions to an ATPSP. For fintechs with limited data sets and a lower risk profile, we recommend that the government sets out a Consumer Driven Banking Security Baseline.
15. Section 37–equivalent requirements should be mapped to existing frameworks (like the RPAA) to avoid redundant audit costs.
16. The Regulations should provide clarity on the requirement of all participating entities to obtain independent third-party confirmation of their security safeguards.
17. Guidelines should provide greater clarity on materiality thresholds for incident reporting, adding definition to the current language requiring reports "as soon as feasible."
18. Assess where RPAA-registered entities have already demonstrated compliance, so open banking accreditation can build on the compliance rather than duplicating it.
19. Define security breach reporting timelines and coordinate notification obligations under other applicable regulations.
20. Clarify the allocation of security responsibilities across participants, including which obligations apply directly to each entity.

21. Clarify expectations for security testing and exercises, particularly as it relates to frequency and scope.

Consent Management

The proposed Regulations stipulate consent-related requirements for participating entities, notably around use of data, renewal triggers, and data deletion.

Fintechs Canada shares the objective of ensuring that consumers are engaging in meaningful consent that does not result in consumer fatigue. To ensure that consent remains meaningful, further clarity would be helpful with respect to trigger renewals. For example, "significant change in circumstance" is vague and, given it will require out-of-cycle consent renewals with a consumer, more specificity is required.

In addition, the regulations should enable a "soft" re-authentication mechanism that allows the firm that originally obtained the customer's consent to renew that consent directly, without requiring the data-holding institution to re-verify the customer's identity each time. We strongly support a proportionate "soft" re-consent mechanism for continued access after the initial consent period, including where consent needs to be refreshed after 12 months or where there is a change in purpose.

Further clarity would be helpful on what is meant by the requirement for the data-providing entity to "authenticate the consumer". It is unclear how this requirement would apply where a recipient subsequently provides data to another participating entity. Requiring the intermediary firm to independently re-authenticate the customer before onward sharing could create significant operational friction. The framework should clarify whether reliance can be placed on authentication already completed by another participating entity.

With respect to identity verification renewal, further clarity is needed on how the data-holding institution is expected to confirm the customer's identity when consent is renewed. For example: is this intended to require the customer to log back into their bank, or could renewal take place solely through the interface of the firm that originally obtained consent? Allowing renewal through that firm's interface is likely to reduce friction and improve renewal rates.

With respect to data that have been irreversibly and permanently modified, the Regulations should stipulate there is no requirement to notify consumers and re-obtain consent for the change, given the data has been anonymized and , in turn, is non-identifiable.

We would welcome additional clarity on how customer disclosure requirements are expected to operate in practice. Depending on when and how the information must be provided, it could introduce additional steps or messaging into the customer journey and create unnecessary friction. The final regulations should allow entities the flexibility to provide this information through appropriate existing channels, such as terms and conditions, privacy notices or help pages, rather than requiring additional disclosures within the consent or authentication journey.

Recommendations:

The regulations should provide clearer guidance and practical examples on consent renewal triggers, including what constitutes a "significant change in circumstance," to preserve meaningful consent while minimizing consumer fatigue and unnecessary friction.

22. Establish a "soft" re-consent mechanism that allows for direct re-authentication.
23. Provide additional clarity for the requirement for the data-providing entity to "authenticate the consumer."
24. Provide clarity on how the data-holding institution is expected to confirm the customer's identity when consent is renewed.

Data Sharing

The proposed Regulations specify circumstances in which an exception to the duty to share data is applied, such as instances where there are reasonable grounds to believe that sharing data would cause physical, psychological or financial harm, or that it would create risks to the security, integrity or stability of the framework or the participating entities' systems.

Fintechs Canada urges for regulatory clarity on the exceptions to share data, particularly with respect to "physical" or "psychological" harm. Similarly, it is not clear which entity decides "reasonable grounds" exist and invokes the exception to

the duty to share, and what recourse a participating entity has should the exemption be applied.

Ultimately, a trusted consumer-driven banking framework must also be a reliable one. If exceptions to the duty to share data are vague or can be used too broadly to deny legitimate data- sharing requests, they risk undermining consumer trust and, in turn, limiting adoption of the framework.

For the framework to support competition, obligations relating to transparency, accountability, and performance should apply symmetrically as between data providers and data recipients. We recommend that the Bank of Canada publish periodic, audited performance metrics for data providers, such as API uptime, average response times, and refusal rates categorized in a defined and enumerated set of refusal reason codes, so that participating entities and the Bank of Canada alike have visibility into whether the duty to share is being met in practice.

Recommendation:

25. Provide further clarity on the exceptions to the duty to share, including what is considered "reasonable grounds" to believe that sharing data would cause "physical" or psychological" harm.
26. The Bank of Canada should require data providers to communicate refusals of a data-sharing request using a defined, enumerated set of refusal reason codes, and should publish periodic, audited performance metrics for data providers, including API uptime, response times, and refusal rates, to ensure the duty to share is applied consistently and transparently.

Screen Scraping

The proposed Regulations are silent on the implementation of a screen scraping ban, as established under the Consumer-Driven Banking Act. Instead, additional consultation will be undertaken on the timeline and parameters of the ban.

Fintechs Canada believes that implementing a screen scraping ban would be premature before Canada's consumer-driven banking framework is fully operational, widely accessible, and demonstrably reliable. Until participants have a clear and workable pathway to accreditation, reliable access to data through prescribed APIs, and sufficient time to transition existing services, removing screen

scraping as an interim access method could disrupt services that consumers and businesses currently rely on.

As the only jurisdiction in the world legislating a ban on screen scraping, it is imperative that this ban does not unintentionally curtail innovation or concentrates risk by creating overdependence on dominant bank APIs.

Ultimately, under a well-functioning and trusted consumer-driven banking framework, screen scraping should not be an easier option to access data than through the prescribed API.

Recommendation:

27. A screen scraping ban should only take effect after a clear transition period during which interim rules apply, and only once the consumer-driven banking framework has demonstrated at least one year of reliable performance and adoption, with accessible pathways for all types of participants.

Liability

The proposed Regulations allocate liability between participating entities based on the activity performed in a given data-sharing transaction: the entity requesting data is responsible for obtaining consumer consent and for securely receiving the data it requests, while the entity providing data is responsible for authenticating the consumer and for securely transmitting the requested data. Under section 53, this division of responsibility is intended to determine which participating entity is liable to the consumer in the event of a direct financial loss arising from a data-sharing transaction.

In practice, however, the grounds for liability as between the requesting and providing entity under section 53 appear to overlap in some scenarios, and the proposed Regulations do not provide guidance on how to determine where a given issue actually originated.

> **Example**: whether a consumer harm arose because the requesting entity mishandled data upon receipt, or because the providing entity transmitted data incorrectly or incompletely in the first place. Without further clarity, participating entities may face genuine uncertainty in situations where the

fault could plausibly sit on either side of a transaction, complicating both internal risk management and the resolution of consumer complaints.

Additional guidance distinguishing between different categories of "fault" would help participating entities anticipate how liability would be allocated in specific circumstances. For example, guidance could usefully distinguish between: faults arising from a deviation from the prescribed technical standard (i.e., where one party's system did not perform in accordance with the specification), and faults arising from a party's failure to act on information reasonably available to it (i.e., where a party received clearly anomalous or erroneous data and had a reasonable opportunity to flag or halt further processing before harm occurred, but did not do so). A framework that considers both where a fault first originated and whether a subsequent party had a reasonable opportunity to prevent resulting harm would provide more predictable outcomes than reliance on the general allocation in section 53 alone.

Similarly, further guidance on consent-related faults would be valuable, particularly with respect to scenarios involving consent scope, consent revocation, and the validity of consent obtained. For instance, it is not clear how liability would be allocated where a requesting entity's data pull exceeds the scope of consent actually obtained, where a consumer revokes consent but that revocation is not promptly reflected across the data-sharing chain, or where consent was obtained in a manner that may not meet applicable legal standards for being freely given and informed. Clear treatment of these scenarios would help ensure liability outcomes are predictable and consistently applied.

Recommendations:

28. The Bank of Canada should provide guidance clarifying how liability under section 53 is to be allocated between requesting and providing participating entities, including how to determine where a fault originated where the grounds for liability as between the two parties appear to overlap.
29. The Bank of Canada should publish a decision-tree or worked-example guidance document addressing common liability scenarios, including deviations from the prescribed technical standard, failures to act on reasonably available information indicating an error, and consent-related faults such as scope overreach, delayed consent-revocation synchronization, and deficient consent collection practices.

Complaints Handling

The proposed regulations refer to complaints procedures, particularly as it relates to the forthcoming designation of an external complaints body. There is limited clarity around complaints and the complaints-handling requirements.

The framework should provide a clear and consistent definition of a "complaint," including whether this captures any expression of dissatisfaction or only matters requiring a formal response. Further guidance should clarify when a complaint is considered received, how complaints submitted through different channels should be identified, and whether service queries, data disputes, fraud reports and technical support issues fall within scope.

The rules should also set out minimum requirements for acknowledging complaints, providing progress updates, issuing final responses and referring consumers to the relevant external complaints body. Clear requirements would reduce inconsistent interpretation and help participating entities design proportionate and effective complaint-handling processes.

Recommendations:

30. The final regulations or accompanying guidance should clearly define what constitutes a "complaint," including whether it includes any expression of dissatisfaction or only matters requiring a formal response, and should clarify when a complaint is considered received across different channels.
31. The rules should establish minimum complaint-handling requirements, including timelines and expectations for acknowledging complaints, providing progress updates, issuing final responses, and referring consumers to the relevant external complaints body.

Violations

The proposed Regulations designate certain provisions as violations subject to administrative monetary penalties, with the maximum penalty set at $1,000,000 for an individual and $10,000,000 for a participating entity or ATPSP. The Bank of Canada retains full discretion in determining the penalty amount for a given violation.

Unlike the sliding scale approach taken by FINTRAC, for instance, which distinguishes violations based on severity, the proposed Regulations do not establish a tiered or severity-based structure for violations under the CDB framework. As currently drafted, the Regulations do not indicate whether a distinction will be made between more and less serious contraventions when penalties are determined, nor do they provide guidance on the factors the Bank of Canada will consider in exercising its discretion.

The framework should clarify whether the $10 million maximum penalty applies to a single underlying incident or separately to each related contravention. Without a clear aggregation rule, one underlying issue could give rise to multiple contraventions and significantly increase the total penalty exposure.

The proposed Regulations also do not specify what opportunity, if any, a participating entity or ATPSP under investigation for a potential violation has to respond or provide context prior to a penalty being determined.

Finally, a breach or contravention under the proposed Regulations may, in some circumstances, also constitute a breach of applicable privacy legislation, giving rise to enforcement exposure under more than one regulatory regime for substantially the same underlying conduct. The proposed Regulations do not address how the Bank of Canada would coordinate with privacy regulators, or other applicable regulators, in such circumstances. Clarity is needed to confirm that participating entities will not face duplicate penalties for substantially the same conduct, and that any enforcement action taken by the Bank of Canada would account for sanctions already imposed by another regulator in respect of the same incident.

Recommendations:

32. The proposed Regulations should provide additional clarity on the treatment of contraventions based on severity, and indicate whether a process will exist for a participating entity under investigation to respond.
33. Clarify the application of the $10 million maximum penalty, and indicate whether it applies to a single underlying incident or separately to each related contravention.
34. The Bank of Canada should clarify how it will coordinate with privacy regulators and other applicable regulators where the same underlying incident gives rise to enforcement exposure under more than one regime, to

ensure participating entities do not face duplicate penalties for substantially the same conduct.

Implementation Timeline and Write-Access

Significant progress has been made in advancing Canada's consumer-driven banking framework over the past several years, and it is important that this momentum continues. After years of consultation, a protracted timeline with limited transparency and clarity for participants will create uncertainty that limits innovation and puts Canadians at a disadvantage.

The draft Regulations estimate approximately $13 billion in monetized benefits for Canadian consumers and SMEs, underscoring that continued delay carries a real cost for consumers, businesses, and Canada's broader economy.

Fintechs Canada calls for greater clarity on timelines around key framework components such as the accreditation process, including the national security review, and reporting requirements. This will help participating entities better understand their obligations for internal planning purposes.

We also underline the importance of moving swiftly to enable write-access. Read-only data access addresses information asymmetry but does not resolve switching friction. Payment initiation, account funding, and pre-authorized debits (PAD) migration are the operational capabilities that make switching practical. If these are deferred to Phase II without an accelerated timeline, the framework's competitive impact will be delayed by years. As such, Phase I should include a pathway to payment initiation.

A material "chain-of-custody" already exists to help support acceleration of write capability. RPAA-registered PSPs already meet rigorous security, fraud, and operational standards to initiate retail payments. The security and accreditation requirements an RPAA-PSP must meet under both the RPAA and CDB frameworks for CDB's Phase 1 (read) should be equivalent to those under Phase II (write), therefore allowing participating entities the capability to initiate consumer-authorized actions safely. This would enable payments initiation to be implemented earlier without requiring a new operational build period or duplicative security accreditation for write-specific functionality.

If the Department determines that write access requires separate or enhanced accreditation criteria, any such criteria should be proportionate and activity-based rather than entity-based. For RPAA-registered participating entities in particular, write-access accreditation should build on the existing RPAA security posture and impose only incremental requirements specific to the risks of action-initiation, such as transaction-specific authentication, fraud monitoring, and consumer-authorization logging. A separate, more onerous accreditation pathway for write access risks entrenching incumbents and undermining fintech participation in Phase II.

As payment initiation under Phase II is expected to execute via the Real-Time Rail (RTR), we urge early and ongoing coordination between the consumer-driven banking framework's governance and RTR governance (Payments Canada), to ensure that: consent obtained under the consumer-driven banking framework is recognized as valid authorization for a corresponding RTR transaction; RTR rules do not conflict with consumer-driven banking data-sharing or action-initiation requirements; and access to the RTR for consumer-driven-banking-accredited participants is streamlined rather than subject to separate, inconsistent criteria.

Taken together, further guidance and specific timelines will enable participating entities to prepare for the necessary build and meet compliance obligations associated with the regime.

Recommendations:

35. Clear guidance, evidence expectations, review timelines, and service standards for key regime components, including accreditation, national security review, and reporting requirements, should be published so participating entities can plan and allocate resources effectively.
36. The regulations should include a firm phase-in calendar for account-type rollout, rather than an open-ended commitment that all accounts will be included eventually, to reduce ambiguity and planning risk for participating entities.
37. Where write-access accreditation criteria are introduced, they should be proportionate and activity-based, building on the existing security posture of RPAA-registered participating entities and imposing only incremental, action-initiation-specific requirements, rather than a separate, more onerous accreditation pathway. The Department of Finance and the Bank of

Canada should coordinate early with Payments Canada to ensure consumer-driven-banking consent is recognized as valid authorization for Real-Time Rail transactions, that RTR rules do not conflict with consumer-driven banking requirements, and that RTR access for accredited participants is streamlined rather than separately gated.

***

Fintechs Canada appreciates the opportunity to provide comments on the proposed Regulations and supports the Government of Canada's continued work to advance a secure, competitive, and consumer-focused consumer-driven banking framework. To realize the full benefits of the regime, including greater consumer choice, improved access to financial services, and stronger innovation across Canada's financial sector, the final Regulations should provide greater clarity, proportionality, and predictability for participating entities.

Fintechs Canada looks forward to continuing to work with the Department of Finance, the Bank of Canada, and other policymakers to ensure Canada's consumer-driven banking framework delivers meaningful benefits for consumers, businesses, and the broader economy.

Thank you again for the opportunity to comment.

Sincerely,

Adriana Vega
Executive Director
Fintechs Canada