CANADA | WHITE PAPER

A Practical Approach to Risk Management in Consumer-Driven Banking

Invela™

Open Finance Covered

Table of contents

Invela™

Open Finance Covered

Invela is an open finance risk management infrastructure provider serving participants including account providers, access aggregators, and data recipients. Invela provides the assessment and risk scoring infrastructure that supports consumer-authorised data sharing. It does not itself participate in those data flows. Invela does not receive, access, or store consumer personal data, consumer financial account information, or consumer authorisation data in connection with the provision of its services.

The observations and recommendations in this white paper are informed by Invela's experience supporting open finance participants across multiple jurisdictions. They reflect Invela's perspective as an infrastructure provider and are offered in that capacity as regulations develop and are implemented under the Consumer-Driven Banking Act.

Executive Summary

Canada's Consumer-Driven Banking Act represents a significant opportunity. As a late mover in open finance, Canada can draw on hard-won lessons from jurisdictions that have already navigated the tension between regulatory oversight and market adoption, and design a framework that avoids the pitfalls of both.

This paper examines the legal and regulatory landscape that shapes consumer-driven banking in Canada, including the Consumer-Driven Banking Act (CDB Act), the Retail Payment Activities Act (RPAA), and OSFI Guidelines B-10 and B-13. It then considers the experiences of Australia and the United States, which illustrate the opposing risks facing Canadian regulators.

Drawing on those experiences, this paper offers two high-level recommendations. First, the Bank of Canada should consider establishing a streamlined, two-tier accreditation framework that focuses regulatory oversight on data aggregators and entities that connect directly to account providers, while delegating responsibility for downstream data recipients. Second, regulators should align the CDB Act and OSFI B-10 by encouraging ongoing risk monitoring through a standardized, market-wide risk scoring framework. This approach would provide meaningful ability to manage ecosystem risk without imposing a prescriptive, ex ante accreditation burden that has stalled adoption elsewhere.

Introduction

There is something to be said for late mover advantage.

Now that it has received royal assent, the Consumer-Driven Banking Act (CDB Act) places Canadian regulators in a relatively enviable position. They have been given a strong legislative mandate to establish one of the world's most comprehensive open finance systems, and they have had the opportunity to learn from others' experiences. Globally, open finance markets have matured considerably over the past decade, with varying degrees of success. Some regulatory approaches (such as Australia's) offer valuable lessons about the risks of over-engineering an open finance regime. Others (such as the United States) offer lessons in the perils of a completely market-driven approach. Canada can learn from both experiences.

Similarly, Invela has benefited from decades of open finance experience in multiple jurisdictions around the world. Based on that experience, we developed the Invela assessment, risk score, and warranty models to address a problem that regulators around the world have struggled with – how to make an open finance system that empowers consumers appropriately legible to regulators without creating an over-engineered regulatory framework that holds back investment and ultimately, consumer adoption.

As Canadian regulators assume their new responsibilities under the CDB Act, this white paper offers an initial, high level perspective on where Canada should go from here as it shifts focus from legislation to regulation. First, we review the legal context, including the CDB Act itself and the existing regulatory framework that will interact with it, with particular attention to the OSFI B-10 Third-Party Risk Management Guideline and the Retail Payment Activities Act (RPAA). Second, we consider how other jurisdictions have approached similar challenges and the opposing risks of over-engineering and underspecifying risk management responsibilities. Finally, we respectfully offer high level suggestions for how Canadian regulators might consider designing the Consumer-Driven Banking framework to balance the goals of consumer empowerment, competition, and risk management.

Legal Context

A. Legislative Framework

Consumer-Driven Banking Act

The CDB Act establishes a comprehensive framework for consumer-directed data sharing with the Bank of Canada as the supervisory authority responsible for overseeing participating entities. The CDB Act applies to data from a broad set of products and services offered to consumers and businesses alike, including deposit accounts, registered and non-registered investment accounts, payment products, lines of credit, mortgages, other loans, and other products and services determined by the Bank of Canada. Substantively, the Act requires participating entities to share consumer data upon valid consumer consent, prohibits charging fees for data sharing, establishes liability obligations, consent requirements, authentication procedures, and breach notices. Importantly, the Act also empowers the Bank of Canada to establish data security rules, and accreditation, registration, and complaints frameworks.[1][2]

The discretion the CDB Act gives to the Bank of Canada in designing an accreditation system is notable. Like several other open finance frameworks, the CDB Act requires entities who wish to participate in consumer-driven banking to be accredited as a bank, financial institution, registered payment service providers, other accredited entity, or third-party service provider. For other registered payment service providers, other accredited entities and third-party service providers in particular, the Bank of Canada's role will be critical in designing substantive requirements for accreditation.

In financial services, The Personal Information Protection and Electronic Documents Act (PIPEDA) has long applied to federally regulated financial institutions and established baseline requirements for consent, access, and data security. However, the recently passed Budget Implementation Act amends PIPEDA to create a new Data Mobility Framework. Under this framework, designated organizations must share individuals' information with third parties upon the individual's request. This amendment creates a general data portability right in Canadian privacy law that complements the sector-specific rights established by the CDB Act.[3]

Retail Payment Activities Act

The Retail Payment Activities Act (RPAA) established a regulatory framework for payment service providers, and seeks to mitigate operational risks in the retail payments sector, safeguard end-user funds, and address national security concerns posed by payment service providers. To these ends, the RPAA imposes obligations on registered payment service providers, including requirements to establish risk management and incident response frameworks, to hold end-user funds in trust accounts or accounts with equivalent protections, and to report incidents that impact end users or the payments ecosystem.[4]

Importantly, the RPAA established a registration framework administered by the Bank of Canada (which the CDB Act now builds upon). Payment service providers must be registered with the Bank of Canada before performing any retail payment activities, and are required when registering to (among other things) describe the activities they perform, list agents and mandataries performing retail payment activities, provide information on end-user funds safeguarding practices, and describe their risk management and incident response frameworks. Unlike the accreditation system called for in the CDB Act, however, the RPAA's registration system leaves little discretion to the Bank of Canada regarding who may be registered. In this way, the CDB Act creates a significantly more complex implementation challenge for the Bank of Canada than the RPAA's registration system did.

B. Regulatory Frameworks & Guidelines

Retail Payment Activities Regulations (SOR/2023-229)

The Retail Payment Activities Regulations (SOR/2023-229) provide the implementing detail for the RPAA's registration and supervision framework. With respect to registration, the Regulations specify the information applicants must provide beyond what the RPAA requires. On risk management, the Regulations require registered PSPs to maintain a written risk management framework that identifies operational risks across eleven specified categories, establishes reliability objectives and targets, includes incident response plans, sets criteria for agents and third-party service providers, and undergoes independent review at least every three years. The Regulations also impose detailed safeguarding requirements for end-user funds and annual reporting obligations. [5]

Third-Party Risk Management Guideline (OSFI B-10)

The Office of the Superintendent of Financial Institutions' (OSFI) Guideline B-10 establishes expectations (not regulatory obligations) for how federally regulated financial institutions manage risks arising from third-party arrangements.[6] B-10 defines 'third-party arrangement' broadly to encompass any arrangement through which a third party provides products or services to a federally regulated financial institution or to its customers on its behalf. [7] Thoughtfully, the CDB Act's obligations for participating entities to conduct ongoing monitoring of third parties appear to echo the B-10 Guidelines, creating an opportunity for Canadian regulators to clarify how third-party risk management principles should apply in the consumer-driven banking context, ensuring that consumer driven banking can achieve both prudential and consumer protection objectives.

Technology and Cyber Risk Management (OSFI B-13)

Guideline B-13 establishes OSFI's expectations for technology and cyber risk management at federally regulated financial institutions. The guideline emphasizes risk identification, assessment, and mitigation through appropriate controls. For consumer-driven banking, B-13's principles regarding secure development practices, access controls, and incident response are particularly relevant for technical standards development. [8]

Balancing Legibility and Adoption

As Canadian regulators take the next steps in designing the CDB Act regulatory framework, they will encounter a familiar tension to other open finance frameworks around the world.

On one hand, the policy goal of consumer-driven banking is clear from its very name – putting consumers in control of their financial data to drive competition and innovation that benefits consumers and the market for financial products and services. In that context, overly complex risk management requirements can impede adoption, disadvantage smaller participants, and ultimately undermine the competitive and consumer benefits that open finance promises to deliver.

On the other hand, financial regulators aren't only interested in competition and innovation. Critical prudential regulatory goals demand that both regulators and financial institutions have sufficient visibility into the ecosystem of firms they interact with to identify and mitigate risks to customers, institutions, and the broader financial system itself. This necessity is increasingly fundamental in the context of increasing digitalization, which brings the potential for data breaches and other cybersecurity risks along with the myriad benefits it provides.

The concept of 'legibility," famously developed by James C. Scott in Seeing Like a State, provides a useful frame for analyzing these tradeoffs. Scott describes legibility as the degree to which a complex system can be read and understood by those who govern it, and his analysis demonstrates the ways in which regulatory efforts to achieve legibility can generate frameworks so elaborate that they become self-defeating. This is a dynamic familiar to observers of open finance regulation around the world. [9]

Regulators reasonably seek to make open finance ecosystems legible so they can identify emerging safety and soundness and consumer protection risks. However, the pursuit of legibility through complex accreditation schemes, prescriptive

technical standards, and comprehensive registration systems can inadvertently create regulatory sludge that slows adoption and defeats the purpose of open finance policies in the first place, further entrenching incumbent advantages.

Of course, there is also danger in systems that ignore legibility altogether in favor of unconstrained consumer adoption. By failing to design targeted systems that mitigate risks to consumers, institutions, and the financial system, regulators risk abdicating their safety and soundness responsibilities and discrediting open finance policies in the long run.

Canada can learn from jurisdictions that have erred in both directions. The challenge is to achieve sufficient legibility for effective supervision without succumbing to the temptation to carefully engineer every detail in advance – recognizing that creating space for the market to respond to directional regulatory incentives may result in both more efficient risk management and greater consumer adoption.

A. Australia: The Risks of Over-Engineering

Australia's Consumer Data Right (CDR) system illustrates the risks of regulatory over-engineering. The CDR (launched in 2020) is a cross-sectoral open finance and data portability framework that requires data holders to share consumer data with accredited recipients upon consumer request. The CDR includes a complex accreditation framework with multiple tiers: unrestricted accreditations, sponsored accreditations, "representative arrangements," and an "outsourced service provider model." Each pathway involves distinct requirements, creating a web of compliance obligations that can be difficult for market participants to navigate and regulators to administer. [10]

Unfortunately, consumer adoption in Australia has been strikingly low. According to a 2024 strategic review commissioned by the Australian Banking Association, only 0.31% of Australian bank customers were actively using CDR at the end of 2023.[11] The review also found that more than half of all data-sharing arrangements initiated under CDR had been discontinued or allowed to lapse, suggesting that even consumers who try the system often do not find sustained value in it.

Notably, a 2022 Statutory Review conducted by the Department of the Treasury identified the CDR's accreditation framework as a significant barrier to consumer adoption. The review found that the CDR's complexity, overly prescriptive requirements, and lack of alignment with existing regulatory regimes were limiting participation and innovation.[12] The review also notes that many market participants report spending more time and resources on compliance than on developing consumer-facing products, and that the accreditation process – along with the division of oversight responsibilities among various regulatory and quasi-regulatory authorities, had created confusion and delay. Importantly, the review concluded that the CDR's accreditation requirements in particular posed a barrier to entry for smaller participants, who lacked the resources to navigate the framework's complexity. In response to the Statutory Review's findings, the Australian government announced a CDR "reset" in August 2024, acknowledging that high regulatory burden and compliance costs had constrained uptake.[13] Among the focus areas of the reset, the government has committed to reducing accreditation costs.

While it is encouraging that the Australian government is reassessing its CDR approach, its experience usefully illustrates the peril of over-indexing to a comprehensively legible open finance regulatory framework.

B. United States: The Risks of Unconstrained Adoption

The United States presents the opposite cautionary tale, as it developed first through market arrangements with regulations coming later. While this approach has driven high consumer adoption rates, it has also created significant confusion among market participants about how to balance prudential and safety and soundness responsibilities with the pro competition and innovation goals of Section 1033 of the Dodd- Frank Act.[14] This confusion creates multiple potential issues for open finance in the United States.[15]

First, the lack of regulatory clarity around the intersection of third party risk management and Section 1033 has created uncertainty for both account providers and third parties. Prudential regulators have issued broad third-party risk management guidance that applies to 'any business arrangement' between regulated institutions and third parties. However, this guidance was not designed for the open finance context and fails to account for the unique dynamics of consumer-directed data sharing.

Second, data aggregators in the US have assumed responsibility for downstream data recipients through contractual flow-down provisions, but these arrangements often lack the operational depth or financial backing to provide meaningful protection. When something goes wrong at the data recipient level, there may be insufficient resources to make consumers or institutions whole.

Third, the slow adoption of technical standards and persistence of legacy access methods like screen scraping have created data quality and security concerns. Many smaller financial institutions continue to be accessed through screen scraping because they lack the resources to build dedicated

APIs. In this context, it may be difficult to know what safety and soundness and consumer protection risks may be present in the system.

The Consumer Financial Protection Bureau's 2024 Personal Financial Data Rights Rule (Section 1033 Rule) represented an effort to address some of these challenges. The rule established consumer data rights and recognized that 'certifications or other identification of fitness to access covered data' issued by recognized standard setters could play a role in determining whether denials of data access are reasonable.[16] However, without clarity on risk management responsibilities from prudential regulators, the ecosystem is held back by fear of both lurking risks and pretextual denials of access by account providers in the name of "risk management."

Recent requests for information from prudential regulators in the US may indicate a new openness to addressing this lack of clarity, providing an opportunity for the US to move forward. However, the longstanding lack of clarity has demonstrated the risk of under-engineering open finance ecosystems in the name of consumer adoption.

Recommendations

Based on our analysis of the CDB Act as part of the Budget Implementation Act, other relevant federal regulations, and the experiences of other jurisdictions, Invela offers the following high level recommendations for Canadian regulators as they develop implementing regulations.

A. Establish a Streamlined Accreditation Framework

The CDB Act provides for accreditation of federal financial institutions, provincial financial institutions, registered payment service providers, other entities, and third party service providers.

Implementing regulations should establish a simple two tiered approach that focuses the Bank of Canada's resources on entities that connect directly to account providers.

TIER 1 **Data Aggregators**

Third party service providers such as data aggregators that facilitate access for numerous downstream data recipients should be the primary focus of the Bank of Canada accreditation system, since they serve as the gateway for the majority of data sharing in the ecosystem and their security and risk management practices directly affect the integrity of the system.

TIER 2 **Direct Participants**

Fintech companies that access consumer data directly from an account provider without going through a data aggregator or other third party service provider should also have direct accreditation obligations from the Bank of Canada. While these entities do not have the potential downstream data recipient risks to contend with that data aggregators do, they also have no one but themselves and the regulator holding them to risk management and data security standards that protect the ecosystem.

Conversely, downstream data recipients who access data indirectly through data aggregators should not require their own Bank of Canada accreditation. The inclusion of these entities, of which there are many, in the Bank of Canada's accreditation framework could begin to replicate the Australian model. Rather, accredited aggregators should be responsible for ensuring their downstream clients meet appropriate standards. Specifically, OSFI B-10 and CDB Act regulations should align to ensure downstream data recipients are appropriately supervised and insured by participating banks and aggregators.

This two-tier structure ensures appropriate regulatory oversight without requiring the Bank of Canada to directly supervise thousands of small fintech companies, leveraging existing market relationships while maintaining accountability.

B. Encourage Ongoing Risk Monitoring & Align CDB Act and OSFI B-10 through Risk Scoring

The CDB Act contains multiple provisions that condition mandatory data access on compliance with other legal requirements. Section 76(1) limits access to cases "unless otherwise prohibited by law," section 79(1) requires compliance with "security safeguards provided for in regulation," and section 82 imposes notification requirements where a data breach could cause "significant harm" to consumers. These provisions create potential tensions with OSFI Guideline B-10, which defines "third-party arrangement" broadly enough to encompass data aggregators and fintechs that connect directly to federally regulated financial institutions. Without clear guidance on how these frameworks interact, banks may face uncertainty about whether B-10 risk management obligations can be invoked to limit or delay data sharing that the CDB Act otherwise requires. This dynamic could, if left unmanaged, replicate some of the market and policy tensions that have emerged in the US.

The Bank of Canada should consider addressing this tension directly in two ways. First, it may be useful to clarify that consumer rights established under the CDB Act cannot be overridden by general risk management guidance. Risk management is essential, but it cannot function as a broad opt-out from consumer-driven banking obligations.

Second, the Bank of Canada should consider encouraging banks to conduct ongoing risk monitoring of participating entities and downstream data recipients with whom they share consumer data. This obligation would align banks' CDB Act responsibilities with their existing duties under B-10, which already requires federally regulated financial institutions to assess and monitor risks arising from third-party relationships throughout the lifecycle of the arrangement.

Finally, to make such ongoing monitoring practical and scalable, the Bank should consider calling for a market-wide risk scoring framework for participating entities and downstream data recipients. A standardized risk score—informed by factors such as accreditation status, security certifications, incident history, and volume of data handled—would render the ecosystem's risk profile legible to both regulators and financial institutions without requiring the prescriptive, ex ante accreditation complexity that has constrained adoption in Australia.

This approach could also achieve substantive alignment between the CDB Act and B-10: banks would meet their prudential obligations through ongoing monitoring rather than by resisting data sharing, and consumers would retain effective access to the data portability rights the CDB Act is designed to provide.

Conclusion

Canada has a rare opportunity to build an open finance framework informed by years of international experience. The core challenge to creating such frameworks is not new, but Canada is unusually well-positioned to get the balance right. The recommendations in this paper – two-tier accreditation structure and a standardized risk scoring framework – are designed to strike that balance. By concentrating direct regulatory oversight where it matters most and empowering market participants to manage downstream risk through ongoing monitoring rather than upfront gatekeeping, Canada can build a Consumer-Driven Banking Framework that is both well-supervised and widely adopted.

Citations

[1] Consumer-Driven Banking Act, as introduced in the Budget Implementation Act, 2025. See Department of Finance Canada, "**Budget 2025: Canada's Consumer-Driven Banking Framework.**"

[2] The selection of a technical standards body has been left to the Department of Finance.

[3] Budget Implementation Act, 2025, **amending** the Personal Information Protection and Electronic Documents Act (PIPEDA), s. 10.4.

[4] **Retail Payment Activities Act**, 2021. See Bank of Canada, **"About Retail Payments Supervision Mandate."**

[5] **Retail Payment Activities Regulations, SOR/2023-229.**

[6] Importantly, provincially regulated institutions may be subject to provincial risk management obligations. While critical, provincial regulations are outside the scope of this paper.

[7] OSFI, **Third-Party Risk Management Guideline** (Guideline B-10), effective May 1, 2024.

[8] OSFI, **Technology and Cyber Risk Management** (Guideline B-13), effective January 1, 2024.

[9] James C. Scott, Seeing Like a State: How Certain Schemes to Improve the Human Condition Have Failed (New Haven: Yale University Press, 1998).

[10] **Competition and Consumer (Consumer Data Right) Rules 2020**. See also ACCC, **CDR Accreditation Guidelines**, Version 6, August 2025.

[11] **Consumer Data Right Strategic Review,** Australian Banking Association, July 2024.

[12] **Statutory Review of the Consumer Data Right,** Department of the Treasury, September 2022.

[13] See Department of the Treasury, **Albanese Government to reset Consumer Data Right,** August 2024.

[14] Dodd-Frank Wall Street Reform and Consumer Protection Act, Pub. L. No. 111-203, § 1033, 124 Stat. 1376, 2008 (2010).

[15] **Open Finance Risk Management White Paper**, Invela, September 2025.

[16] CFPB, **Personal Financial Data Rights Rule** (Final Rule), 89 Fed. Reg. 96,416 (November 18, 2024).