



Canadian Securities
Administrators

Autorités canadiennes
en valeurs mobilières

CSA Collaboratory

Data Portability Project

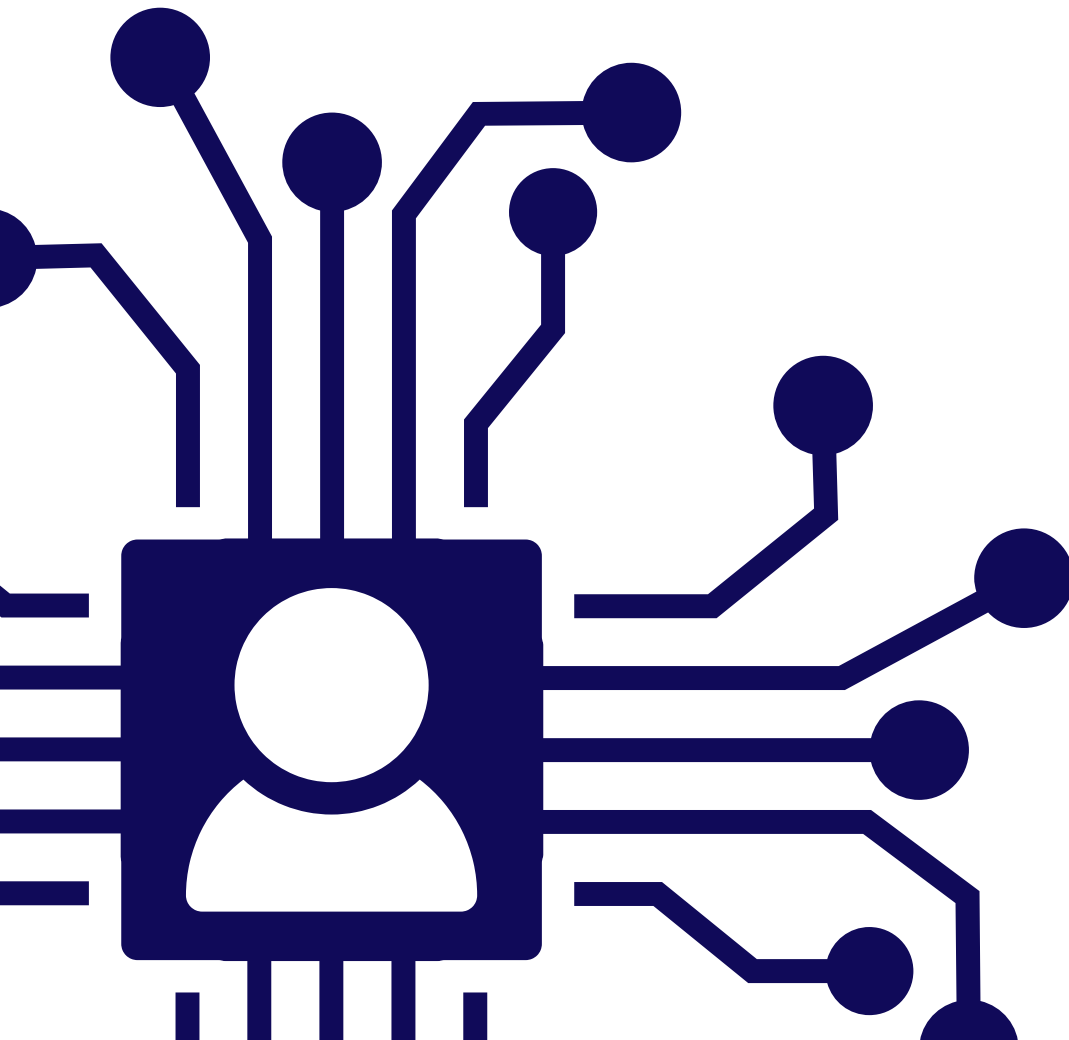


Table of content

Executive Summary	3
1. Data Portability Project Background and Objectives	4
1.1 CSA FinHub & Collaboratory	4
1.2 Canadian Consumer-Driven Banking Framework	4
1.3 Data Portability Project Phases	5
1.4 Data Portability Project Objectives	5
2. Phase 1: Discussion Paper and Stakeholder Feedback	6
3. Phase 2: Industry Roundtables and Quebec Meetings	7
3.1 Vancouver Forum – May 2025	7
3.2 Calgary Forum – September 2025	7
3.3 Quebec Bilateral Meetings – December 2025 to January 2026	7
4. Stakeholder Feedback: Key Themes and Insights	8
4.1 Legal and Regulatory Barriers to Adoption	8
4.2 Privacy, Security, and Consent Management	9
4.3 Data Scope and Boundaries	9
4.4 Data Portability Implementation Models	9
4.5 Business Incentives and Market Dynamics	11
5. Decision on Phase 3: Live Testing Environment	11
6. Key Learnings and Recommendations from Stakeholders	12
6.1 Key Learnings as expressed by stakeholders	12
6.2 Stakeholder Recommendations	13
7. Conclusion	13
Questions	14

Executive Summary

The CSA Collaboratory Data Portability Project (the Data Portability Project) is an initiative by the Canadian Securities Administrators (CSA) to explore how data portability can enhance investor control over personal data, particularly in the context of electronic Know-Your-Client (e-KYC) portability, while maintaining market integrity and investor protection.

While the Collaboratory is supported by all CSA members, not all jurisdictions participate in each initiative. The Ontario Securities Commission did not participate in the data portability project.

Key Definitions

In this report, we use the terms below as follows:

Data Portability means a person can ask an organization to transfer them their personal data—or send it to another organization—in a standard digital format that's easy to use. This can be a one-time transfer or happen on an ongoing basis.

e-KYC (electronic Know-Your-Client) refers to when a firm collects and verifies KYC information using digital tools, such as online forms, electronic documents, or automated checks, thereby assisting the firm in performing its KYC obligations and suitability assessment.

Launched under the CSA Financial Innovation Hub's (FinHub) Collaboratory in early 2025, the Data Portability Project unfolded in two phases: a discussion paper and comment period (Phase 1), and a series of industry roundtable meetings and bilateral meetings (Phase 2). It also contemplated a third phase, a live testing environment, if warranted (Phase 3). The Data Portability Project engaged a wide range of stakeholders across Canada—including registered firms, financial institutions, fintechs, law firms, academics, regulators, and investor advocates—to identify opportunities and challenges associated with enabling investors to securely and efficiently transfer (i.e. port) their data between financial service providers.

Stakeholders generally expressed broad support for the Data Portability Project, and recognized the potential for data portability to reduce duplication in KYC processes and improve investor experience. However, they also raised concerns about regulatory uncertainty, privacy and consent management mechanisms, data security, and the need for data standardization. This report summarizes input received from stakeholders during Phases 1 and 2, including key learnings and recommendations based on that feedback. The insights gathered from Phases 1 and 2 may help inform the CSA's future rule-making, guidance, policy development, and supervisory efforts.

1. Data Portability Project Background and Objectives

1.1 CSA FinHub & Collaboratory

The FinHub supports innovation in Canadian capital markets by examining new and emerging technologies and business models and considering their regulatory implications. Within the FinHub, the CSA established the Collaboratory, which is a themed cohort-based mechanism where participants can explore and test new financial concepts, technologies, regulatory approaches, or innovative business models in capital markets, within a controlled and regulatory-flexible framework, and with guidance from CSA staff.

The Data Portability Project is the inaugural Collaboratory theme. It focuses on how investors' personal and financial data could be securely and efficiently ported between registrants (including through an e-KYC service provider) at the investor's request (e-KYC portability). This theme was selected after considering evolving international and domestic privacy laws and open finance initiatives, including the Canadian Consumer-Driven Banking Framework (described below), that seek to empower consumers with greater control over their data. In Canadian securities markets, data portability could significantly impact e-KYC processes by reducing duplication and friction when clients move between registered firms.

1.2 Canadian Consumer-Driven Banking Framework

Canada's Consumer-Driven Banking Framework (CDB Framework) is the federal regime that will let Canadian individuals and businesses share their financial data with participating entities of their choice. Established under the Consumer-Driven Banking Act,¹ the CDB Framework will initially be mandated for specified large banks that meet a threshold for retail volume. Other regulated financial institutions and entities will be able to opt in, provided they meet accreditation requirements. Participating entities may use accredited-third party service providers to outsource certain tasks, including the movement of data. On June 27, 2026 (after completion of Phases 1 and 2 of the Data Portability Project) the federal government published proposed Consumer-Driven Banking Regulations for consultation, providing additional detail regarding accreditation, consent, security, and other operational aspects of the framework.² The CDB Framework is not yet fully operational, as the proposed regulations remain subject to consultation and finalization, and additional technical standards are still being developed. A phased rollout is underway, beginning with "read-only access" data sharing, followed by additional functionalities such as payment initiation and account switching ("write-access") in a later regulatory phase.³

¹ [Consumer-Driven Banking Act](#) (S.C. 2026, c. 3, s. 224).

² [Canada Gazette, Part 1, Volume 160, Number 26: Consumer-Driven Banking Regulations](#)

³ All information in this document regarding the CBD Framework is based on publicly available data as of the date of publication of this Report and may be superseded by updated information as and if released by the federal government or applicable federal agencies.

1.3 Data Portability Project Phases

The timeline below summarizes the key activities and milestones:

- Phase 1 – Discussion Paper and Comment Period (February–May, 2025): CSA Multilateral Discussion Paper 11-406 – *CSA Financial Innovation Hub Introduces Collaboratory and Data Portability Test* was published on February 18, 2025, to introduce the Collaboratory, the data portability theme, and to solicit written feedback from stakeholders.
- Phase 2 – Industry Roundtable Meetings and Bilateral Meetings (May 2025–January 2026): Roundtables were held in Vancouver and Calgary, and bilateral meetings were hosted in Montreal.

A live testing environment was contemplated as a potential Phase 3, to be undertaken only if necessary and appropriate based on the outcomes of and feedback from Phases 1 and 2. As a result of stakeholder consultations, CSA staff decided not to proceed with phase 3 at this time.

1.4 Data Portability Project Objectives

In Phases 1 and 2 of the Data Portability Project, CSA staff set out to:

- Understand how data portability (and in particular, e-KYC portability) might affect compliance with Canadian securities laws, self-regulatory organization rules, privacy obligations, and market efficiency.
- Explore technological solutions (e.g. digital identity wallets and blockchain) and assess different implementation models, including centralized and decentralized.
- Determine whether a Phase 3 live testing environment would be necessary and appropriate.

In meeting these objectives, CSA staff engaged with diverse stakeholders to gather perspectives on opportunities, challenges, and a potential securities regulatory role in the data portability space. These objectives align with the [CSA's 2025–2028 Business Plan](#) (Strategic Goal 3.2), which emphasizes building regulatory capacity for emerging digital business models and supporting innovation through cohort-based testing environments.

2. Phase 1: Discussion Paper and Stakeholder Feedback

Multilateral Discussion Paper 11-406 - *CSA Financial Innovation Hub Introduces Collaboratory and Data Portability Test* introduced the Collaboratory and the data portability theme, outlined potential e-KYC portability scenarios, and posed 23 consultation questions. These questions asked stakeholders to provide feedback to the CSA on topics including potential regulatory barriers, privacy and consent issues, data standards, and the CSA's potential regulatory role in or response to data portability solutions.

The CSA received 21 comment letters. Respondents included industry associations, fintechs, financial institutions, investment firms, investor advocates, and legal experts, among others. Key themes included:

- Support for the Data Portability Project.
- Recognition of the potential of e-KYC portability to make KYC processes more efficient and improve investors' experiences.
- Concerns about regulatory uncertainty, particularly around the delegation of KYC collection and the requirement for "meaningful interaction" with clients, regardless of tools or technology, that is contained in the Companion Policy to National Instrument 31-103 *Registration Requirements, Exemptions and Ongoing Registrant Obligations* (CP 31-103).
- Emphasis on privacy and consent, with suggestions for client consent dashboards and alignment with Quebec's Law 25, which amended the *Quebec Act respecting the protection of personal information in the private sector*.
- Calls for standardized data formats and application programming interfaces (APIs) to enable interoperability.
- Recognition of the need for cross-sector coordination, particularly with the federal CDB Framework and related initiatives.

3. Phase 2: Industry Roundtables and Quebec Meetings

Building on Phase 1, CSA staff held two roundtable meetings hosted in Vancouver and Calgary and conducted bilateral meetings in Quebec.

3.1 Vancouver Forum – May 2025

The Vancouver forum brought together over 200 participants. Discussions focused on:

- Regulatory barriers preventing the development of data portability in Canada.
- Privacy and consent and how concerns around these issues could be mitigated in a data portability testing environment.
- Technology models to implement data portability solutions in Canada.
- The design of a potential Phase 3 live testing environment.

3.2 Calgary Forum – September 2025

The Calgary forum included around 100 participants. Key themes included:

- The need for guidance on the application of KYC delegation and meaningful interaction requirements as addressed in National Instrument 31-103 *Registration Requirements, Exemptions and Ongoing Registrant Obligations* (NI 31-103) or CP 31-103, in the context of data portability.
- Potential data portability implementation models, together with the advantages and disadvantages of such models.
- Concerns about liability and trust in third-party e-KYC service providers.
- The importance of investor consent mechanisms, such as user-friendly consent dashboards.

3.3 Quebec Bilateral Meetings – December 2025 to January 2026

In recognition of Quebec's unique privacy regime under Law 25, CSA staff decided to hold Quebec meetings in the form of bilateral meetings with 15 stakeholders, including large financial institutions, investor and dealer advocacy groups, exchanges, and others.

Key themes included:

- General preference for data portability implementation models that allow for simplicity and accountability, such as a single central hub that oversees data collection, storage, and verification.
- Emphasis on aligning securities regulation with Quebec's Law 25.
- Concerns about duplicative efforts if provincial securities law standards diverge from federal CDB Framework standards.

4. Stakeholder Feedback: Key Themes and Insights

4.1 Legal and Regulatory Barriers to Adoption

Data portability can streamline and optimize the KYC process, but some market participants shared reluctance to implement data portability solutions for regulatory compliance reasons.

A central concern across Phases 1 and 2 feedback was uncertainty as to how Canadian securities laws would apply to data portability, particularly regarding KYC-related obligations under NI 31-103. In particular, stakeholders highlighted section 13.2 of CP 31-103, which states the following:

KYC obligations cannot be delegated

Responsibilities arising from the KYC obligation cannot be delegated. A registrant may not rely on a third party, such as a referral agent, for KYC information.

Stakeholders emphasized that because firms must retain full responsibility for compliance, the KYC process is not easily delegated. Stakeholders also identified that neither NI 31-103 nor CP 31-103 are clear on whether sending and receiving KYC information through utilities such as a data portability service provider would contravene the delegation restrictions. Some firms reported that they had sought legal opinions to determine whether they were fulfilling KYC obligations when outsourcing KYC collection to a third party.

Stakeholders also consistently sought clarity on whether using an external data portability service would violate rules requiring a “meaningful interaction” with clients to fulfill KYC obligations. In particular, stakeholders highlighted section 13.2 of CP 31-103, which states the following:

Meaningful interaction with the client regardless of tools or technology

The process of collecting and updating a client’s KYC information must amount to a meaningful interaction between the client and the registrant. Although standardized questionnaires or other tools may be used to facilitate the collection of KYC information and to document that information, the registrant remains responsible for the KYC process. The KYC obligation does not vary depending on the medium through which a registrant interacts with its client to gather the necessary information.

Stakeholders identified uncertainties as to whether using a data portability solution would allow a registrant to comply with the meaningful interaction requirements and restrictions. An example provided was a situation where a registrant’s client consents to transfer of information directly to the registrant from third party data sources, and a KYC questionnaire is used that is pre-populated for the client’s review with this information.

4.2 Privacy, Security, and Consent Management

Stakeholders emphasized that investor consent should be explicit, revocable, and easy to manage, and that data sharing should cease when the relationship ends or otherwise has lapsed in accordance with clear and unambiguous consent. The concept of a “consent dashboard” emerged as a potential method by which investors could provide or withdraw such consent. A dashboard would allow investors to view and manage data-sharing permissions. Quebec participants highlighted Law 25’s requirements for clear, time-limited consent, and suggested alignment with Law 25’s model.

Stakeholders also emphasized the importance of data minimization principles, meaning ensuring that only necessary data is collected and shared. Registrants may be concerned with transferring data such as proprietary information, specific transaction histories that could provide insight into client investment strategies, or internal risk ratings.

Stakeholders emphasized **security** as a priority. For example, stakeholders suggested that the CSA may consider introducing clear standards or certifications for data portability providers. Stakeholders also stressed the need for encryption, audit logging, and oversight of third-party vendors.

CSA staff acknowledge the importance of data security and security protocols given the risk of data breaches as data becomes more portable between firms. While data portability enables consumers to direct the transfer of their financial information between institutions and service providers, greater volumes and frequencies of data transfers can broaden the potential attack surface and increase the likelihood of unauthorized access, interception, or misuse.

4.3 Data Scope and Boundaries

There was general agreement among stakeholders that only raw, factual client-provided data should be required to be ported, and not firms’ proprietary assessments or derived analytics. Many stakeholders emphasized that portability should focus on objective data (e.g., name, address, investment objectives, or portfolio composition), while internal investor profiles, risk ratings or suitability assessments should remain with the originating firm. This feedback is consistent with many current open finance frameworks, which scopes in raw, consumer-provided or transaction-level data, but excludes data that is enhanced by a participating entity to significantly increase its usefulness or commercial value, often referred to as derived data.

4.4 Data Portability Implementation Models

Stakeholders discussed a range of potential data portability implementation models. While participants frequently referred to “centralized” and “decentralized” approaches, those terms were at times used to describe fundamentally different concepts. Feedback received on data portability models generally fit within four categories: (i) central mandated utility, (ii) market-driven peer-to-peer systems, (iii) third-party intermediaries or aggregators, and (iv) centralized data repositories or warehouses. The feedback did not result in a clearly preferred single implementation model. Rather, participants described potential benefits and challenges

associated across approaches and emphasized the importance of security, investor consent, interoperability, accountability, and trust, regardless of the underlying architecture.

Model 1 – Central Mandated Utility / Government Controlled Infrastructure

Several stakeholders, including investment managers, fintechs, and certain industry associations, discussed or supported models involving a regulator-mandated or government-supported utility operating under common standards. Participants noted that such a model could provide a single point of accountability, facilitate investor consent management, simplify compliance obligations, and promote interoperability through standardized data formats and processes. Some stakeholders suggested that existing government platforms or open banking-style frameworks could provide a foundation for such an approach for data portability. Others emphasized the importance of accreditation, certification, or regulator recognition in establishing trust and encouraging adoption.

Some financial service firms, fintechs, and crypto-asset platforms, among other stakeholders, identified potential challenges associated with a centrally mandated model. Concerns included cybersecurity risks arising from concentration of data, the potential creation of a single point of failure, governance considerations, and questions regarding investor trust if a single entity were responsible for managing or facilitating access to sensitive KYC information.

Model 2 – Market-Driven Peer-to-Peer Data Sharing

Some stakeholders, such as technology consultants, e-KYC service providers, and certain fintech participants, expressed support for market-driven approaches that could allow firms or investors to share information directly using APIs or distributed network architectures. Participants supporting this infrastructure emphasized flexibility, competition, and reduced reliance on a single provider or point of contact. Several stakeholders suggested that market participants may be better positioned than the government or regulators to develop technical solutions that respond efficiently to industry needs.

Technology and fintech participants also noted that certain decentralized technologies may create implementation challenges. Some stakeholders questioned whether blockchain-based architectures are appropriate for digital identity or e-KYC use cases, and raised concerns regarding governance, accountability, and regulatory oversight within distributed systems. Others noted that peer-to-peer data sharing approaches may require firms to independently interpret consent requirements and other legal requirements, potentially resulting in inconsistencies in interpretations across participants.

Model 3 – Third-Party Aggregators and Intermediaries

Fintechs, financial institutions, and other market participants discussed models in which independent service providers facilitate the exchange of client information between participants. Under these approaches, intermediary organizations may validate, interpret, transmit, or otherwise support the movement of information. Stakeholders supporting this type of model emphasized that competition among service providers can encourage innovation and reduce concentration risk associated with a single utility. Some fintechs highlighted models in which the intermediary facilitates portability without necessarily retaining the underlying data, thereby reducing cybersecurity concerns associated with centralized storage. Financial institutions and

other stakeholders also observed that intermediary-based models would require clear standards relating to security, accountability, operational resilience, oversight, and liability

Model 4 – Centralized Data Repositories and Warehouses

Exchanges, financial services firms, and service providers referenced models involving centralized repositories that collect or maintain information from multiple market participants and provide access when authorized by the client. Examples discussed included data warehouses and industry utilities that aggregate information to reduce duplication and improve operational efficiency. Stakeholders noted that these models may create efficiencies by allowing information to be updated in a single location while maintaining an audit trail of access and changes.

These stakeholders also acknowledged that repository-based approaches require careful consideration of cybersecurity, governance, and concentration risk given the volume and sensitivity of information maintained within a centralized environment. Several participants specifically noted concerns about creating a single target for cyber-attacks and the need for strong security controls.

4.5 Business Incentives and Market Dynamics

Stakeholder views differed on whether data portability obligations in the investment market should be implemented through a provincial regulatory mandate or through market forces. There was general agreement that broad adoption may require legislative changes in order to compel relevant market participants to implement data portability processes.

Incentives to adopt data portability solutions may differ between types and sizes of institutions. For instance, some stakeholders identified that larger institutions may have less incentive to streamline the sharing of their clients' data. However, the reduction in onboarding friction was generally viewed as a positive for smaller firms. The general consensus was that investors would be the stakeholder group that benefits most from data portability implementation.

5. Decision on Phase 3: Live Testing Environment

CSA staff considered the feedback from the Phase 1 and 2 consultations and decided not to proceed with a Phase 3 live testing environment at this time. This decision reflects careful consideration of stakeholder feedback, practical implementation challenges, and the broader regulatory landscape at the present time.

Stakeholders identified several reasons for not proceeding with a live testing environment:

- Some participants in Phase 2 expressed reluctance to participate in a live test without alignment with the federal CDB Framework initiative. Premature standardization could lead to inefficiencies and fragmentation. Because the proposed CDB Framework regulations will establish more detailed foundational standards for data portability across the financial sector, waiting for their full implementation and operation may be beneficial.
- Limited interest from major institutions in participating in a live testing environment.

- Practical challenges for registrants, including resource constraints and lack of data standardization.

6. Key Learnings and Recommendations from Stakeholders

6.1 Key Learnings as expressed by stakeholders

1. **Data Portability Can Reduce Friction in Client Onboarding**
Stakeholders emphasized that data portability has the potential to reduce friction for investors who are switching providers or opening multiple accounts, and reduce friction experienced by registrants during client onboarding processes. Staff note that this feedback on potential implications for Canadian investors is consistent with a growing body of empirical evidence noting increased utilization of open banking and open finance initiatives globally.⁴
2. **Federal Alignment Is Critical**
Stakeholders emphasized that securities-specific data portability should be built on the foundation of the CDB Framework. The CSA proceeding without alignment with the federal framework risks fragmentation and inefficiencies.
3. **Investor Protection and Security Considerations Are Necessary**
Stakeholders emphasized that any data portability solution must include strong privacy protections and robust cybersecurity measures, and must maintain the integrity of KYC obligations. Consent must be clear and revocable, and data minimization principles should apply.
4. **Regulatory Guidance Could Help to Enable Progress**
Clarification on how current securities regulations—particularly KYC obligations—apply in this data portability context could help realize benefits. Some stakeholders noted that uncertainty around delegation and meaningful interaction may be a barrier to data portability implementation.
5. **Technology Solutions Exist—Implementation Is the Challenge**
The technology to enable data portability already exists. Stakeholders emphasized that the implementation challenges primarily lie in standardization, integration with firm workflows, and ensuring compliance with regulatory and privacy requirements.
6. **No Clear Consensus on a Single Data Portability Implementation Model**
While some stakeholders preferred models featuring centralized governance or oversight because of accountability, standardization, and investor protection considerations, others favoured market-driven or intermediary-based approaches that promote competition and reduce reliance on a single infrastructure provider. Feedback suggested that

⁴ For instance, see “*Opening Doors to Open Finance: Evidence from the International Experience.*” *BIS Papers No. 168. Basel: Bank for International Settlements, 2024*, p.6, which noted an increase in the number of open finance users and an increase in open finance API calls.

governance, security, consent management, and interoperability are the most important considerations in selecting a preferred model.

6.2 Stakeholder Recommendations

During Phases 1 and 2, stakeholders provided a number of recommendations to CSA staff for further consideration, which included:

1. **Monitor Federal CDB Framework**
CSA staff should continue to monitor federal consumer-driven banking legislative and policy development and continue to consider opportunities to engage and align with federal policymakers and industry on securities-regulatory related considerations.
2. **Consider Clarifications on KYC Obligations in a Data Portability Context**
The CSA should consider clarifying the application of KYC obligations when client data is transferred through data portability service providers, while maintaining adequate protections for investors.
3. **Monitor Industry Standards Development Related to Data Portability**
The CSA should continue to monitor the development of data standards, including data formats, API specifications, security certifications, and consent management protocols. If appropriate, CSA staff should consider participating in the development of such standards through live testing or other tools, such as a synthetic dataset.

7. Conclusion

The Data Portability Project has generated valuable insights and considerations regarding data portability for the CSA. The Data Portability Project engaged diverse stakeholders and explored the opportunities, challenges, and regulatory considerations associated with enabling investors to utilize data portability solutions to transfer their data between financial service providers. Engagement included various forms of consultation: 21 written submissions, two focused roundtable forums, and multiple bilateral meetings, hosted across Canada.

Based on feedback received from Phases 1 and 2, CSA staff have decided not to proceed with a Phase 3 live testing environment at this time. This decision reflects the practical realities facing market participants and the importance of coordinating with broader financial services data frameworks. Instead, the CSA will use the feedback gathered to inform its rulemaking, supervisory, and policy functions as the data portability landscape evolves. CSA staff expect to continue to monitor developments related to Data Portability. If warranted, CSA staff expect to engage further with market participants on this topic as the data portability ecosystem and related legislative structures evolve.

Questions

Please refer your questions to any of the following:

British Columbia Securities Commission

Khalil Jessa
Senior Legal Counsel,
Capital Markets Regulation
kjessa@bcsc.bc.ca

Elliott Mak
Senior Legal Counsel,
Corporate Finance
emak@bcsc.bc.ca

Alberta Securities Commission

Mohamed Zohiri
Legal Counsel and FinTech Adviser
Advanced Research and Knowledge
Management (ARKM)
Mohamed.Zohiri@asc.ca

Chelsea Tolppanen
Legal Counsel
Advanced Research and Knowledge
Management (ARKM)
Chelsea.Tolppanen@asc.ca

Autorité des marchés financiers

Bruno Vilone
Director, Asset Management Policy and
Technological Innovation
Asset Management
bruno.vilone@lautorite.qc.ca

Financial and Consumer Affairs Authority of Saskatchewan

Caroline Smith
Senior Legal Counsel
Securities Division
caroline.smith@gov.sk.ca

Financial and Consumer Services Commission of New Brunswick

Jake Calder
Manager of Policy
Securities
Jake.Calder@fcnb.ca

Nova Scotia Securities Commission

Cynthia Tambago-Alday
Deputy Director,
Registration & Compliance
Cynthia.Tambago-Alday@novascotia.ca

Manitoba Securities Commission

Chris Besko
Executive Director
chris.besko@gov.mb.ca