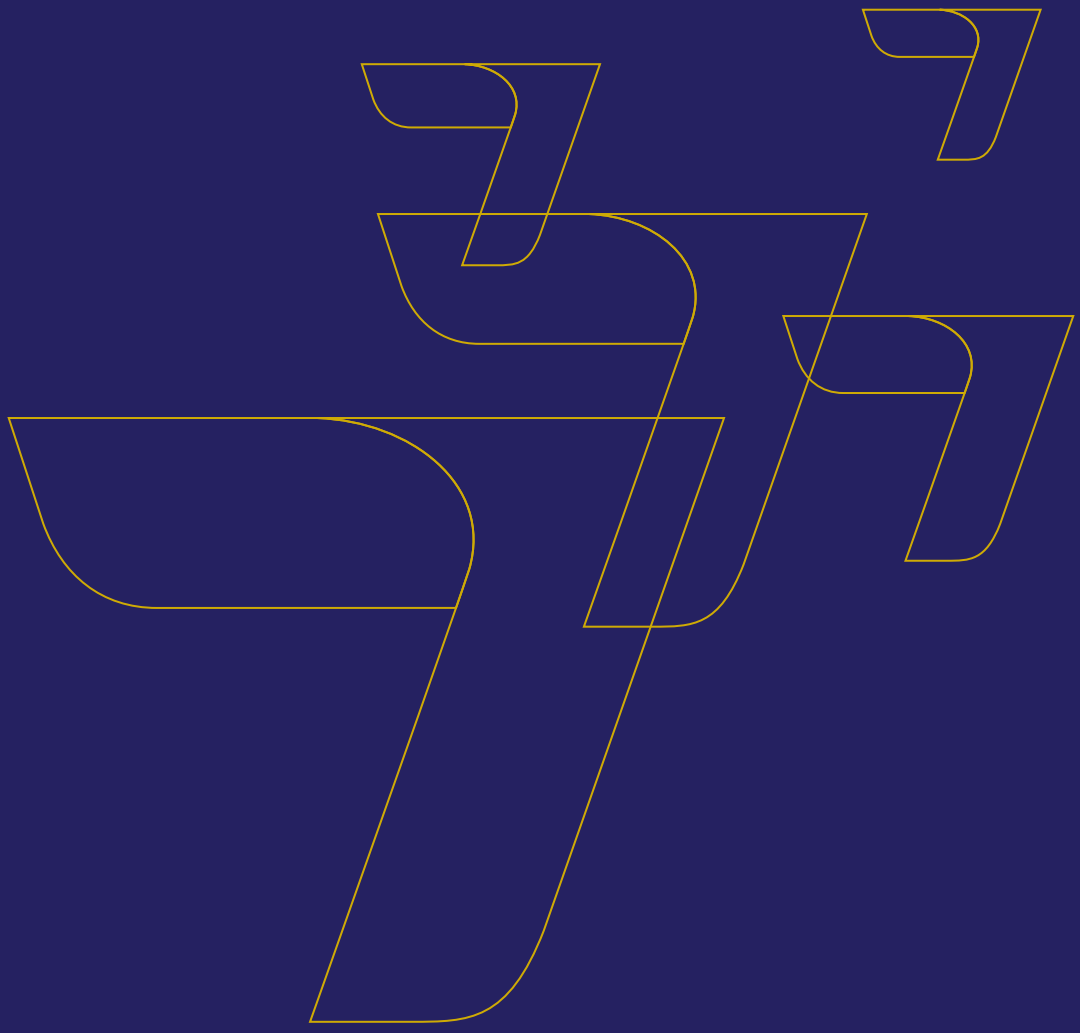
SIMA Securities and Investment Management Association

AMVI Association des marchés de valeurs et des investissements

Submission

Re: CSA Multilateral Discussion Paper 11-406 – CSA Financial Innovation Hub *Introduces Collaboratory and Data Portability Test*

May 16, 2025



ANDY MITCHELL
President and CEO *Président et chef de la direction*
amitchell@sima-amvi.ca 416 309 2300

May 16, 2025

Delivered via website (https://www.securities-administrators.ca/consultations/)

British Columbia Securities Commission
Alberta Securities Commission
Financial and Consumer Affairs Authority of Saskatchewan
Manitoba Securities Commission
Financial and Consumer Services Commission of New Brunswick
Superintendent of Securities, Department of Justice and Public Safety, Prince Edward Island
Nova Scotia Securities Commission
Office of the Superintendent of Securities, Service NL
Northwest Territories Office of the Superintendent of Securities
Office of the Yukon Superintendent of Securities
Nunavut Securities Office

Dear Sirs and Mesdames:

RE: CSA Multilateral Discussion Paper 11-406 – CSA Financial Innovation Hub *Introduces Collaboratory and Data Portability Test*

The Securities and Investment Management Association (SIMA) appreciates the opportunity to comment on CSA Multilateral Discussion Paper 11-406 – CSA Financial Innovation Hub *Introduces Collaboratory and Data Portability Test* (the **Discussion Paper**).

SIMA empowers Canada's investment industry. The association, formerly the Investment Funds Institute of Canada (**IFIC**), is now the leading voice for the securities and investment management industry. The industry oversees approximately $4 trillion in assets for over 20 million investors and participates in the Canadian capital markets. Our members – including investment fund managers, investment and mutual fund dealers, capital markets participants, and professional service providers – are committed to creating a resilient, innovative investment sector that fuels long-term economic growth and creates opportunities for all Canadians.

We operate within a governance framework in which we gather input from our member working groups. The analyses and recommendations of these working groups are submitted to the SIMA board or board-level committees for direction and approval. This process ensures submissions that reflect the input and direction of a broad range of SIMA members.

Summary

SIMA welcomes regulatory initiatives aimed at improving the investor experience and reducing barriers to investor engagement. Overall, SIMA supports the CSA's examination of data portability[1], e-KYC[2] and e-KYC portability[3] solutions in the Canadian capital markets and its plan to conduct industry consultation through its new forward-looking cohort-based testing environment.

This letter outlines preliminary guiding principles and recommendations to help inform the CSA's consideration of data portability and e-KYC solutions. As the topics in the Discussion Paper are in the early stages of consideration, the guiding principles and recommendations in this letter are subject to change. Appendix A contains responses to certain questions posed in the Discussion Paper. Appendix B contains the CSA's Test Overview as reference.

Scope and key terms

The response letter focuses on client-initiated data portability and provides general commentary regarding e-KYC and e-KYC portability solutions.

Our response letter is based on the following assumptions about the data portability eco-system:

a. a data holder means a securities registrant with an account for a client, or a related or third party acting on behalf of the securities registrant for the client's account;

b. a data recipient means a securities registrant or a third party authorized by a securities registrant or a client to receive the client's data; and

c. client data may be stored (i.e. data centre) during transmission to facilitate data portability or the data could be transferred without storage.

Guiding principles

SIMA shares the preliminary guiding principles below to inform the analysis and responses:

1. Ensure privacy considerations are appropriately addressed.

2. Ensure harmonization and consistency, where applicable, with federal and provincial initiatives relating to data portability and consumer-driven banking to align with the overall goal of reducing regulatory burden and maintaining efficiency.

3. Ensure all CSA members participate in rule making for data portability and e-KYC solutions to promote harmonization and minimize regulatory burden.

4. Use meaningful mechanisms designed to ensure clients understand they are sharing information (through a data holder) with data recipients and the subsequent use of the data by such recipients.

5. Develop a definition of data and derived data in consultation with industry which will inform future phases.

6. Address the extent and apportionment of liability and responsibility for data holders and data recipients from regulatory investigations, audit findings and enforcement actions. This is to address concerns from

---

[1] The Discussion Paper defines Data Portability to mean the ability of individuals to request that a data holder transfers to them or a specific third party, data concerning that person in a structured, commonly used, and machine-readable format on an ad hoc or continuous basis. The definition is based on the 2024 OECD report on the impact of data portability on user empowerment, innovation, and competition.

[2] The Discussion Paper defines **e-KYC** as the process of collecting a client's information and, completing identity verification and other KYC requirements as set out in section 13.2 of National Instrument 31-103 *Registration Requirements, Exemptions and Ongoing Registrant Obligations* (**NI 31-103**) using digital means, such as through electronic forms, digital documents, and varying degrees of automation. This enables the registrant to obtain information about the client that assists in performing its KYC obligations and a suitability assessment as set out in 13.3(1)(a)(i) of NI 31-103.

[3] The Discussion Paper defines e-KYC portability to mean the ability for individuals to obtain, reuse and port financial and other personal information from one financial service provider to another for purposes of facilitating the process to gather client information under the KYC process across different securities registrants that are providing investment services and/or products to the individual.

securities registrants with potential liability associated with participating in data portability and e-KYC solutions, and accordingly, are looking to securities regulators to help mitigate.

7. Proceed in phases with any testing and implementation of data portability and e-KYC solutions, consistent with the CSA's phased approach to the data portability test outlined in the Discussion Paper.

Recommendations

Based on a review of the Discussion Paper, SIMA recommends the following preliminary considerations:

1. **Privacy considerations**: the CSA regulatory framework for data portability and e-KYC solutions needs to address privacy concerns associated with sharing client data with various parties, such as data centres and data recipients. Potential approaches to addressing privacy concerns include:
    a. implementing robust client authorization mechanisms to ensure clients are fully informed and able to provide meaningful authorization to data holders for the transfer of their data through a data portability solution;
    b. implementing robust client consent mechanisms to ensure clients are fully informed and able to provide meaningful consent to data recipients for the collection and use of their data through a data portability solution; and
    c. establishing clear guidelines on data portability options for clients.

2. **Regulatory burden and mitigants**: it is important for the CSA to consider whether the implementation of data portability and e-KYC solutions could inadvertently create regulatory burden on securities registrants. Individual rights for data portability will need to be balanced with the practicalities of existing securities law requirements for account opening, KYC and suitability. The regulatory framework for data portability and e-KYC portability should seek to reduce the potential regulatory burden on securities registrants through various approaches, including:
    a. at the outset, limiting the scope of data to be provided for the purposes of client identification;
    b. determining the extent of liability and responsibility for data holders and data recipients for the management of regulatory risk and potentially legal risk;
    c. as applicable, aligning data portability solutions with developing standards for data portability at federal and provincial levels to ensure consistency and harmonization where appropriate for securities registrants; and
    d. providing clear guidance on how registrants can utilize data portability and e-KYC solutions while complying with securities legislation, and if necessary, amending existing securities laws, rules and guidance, for example, in the context of account transfers.
3. **Phased approach:** pursuing a phased approach to considering data portability and e-KYC solutions to ensure careful examination of key issues including privacy concerns and regulatory burden. In addition, a phased approach is useful in identifying where rules or policies may need to pivot in direction or focus if certain challenges or obstacles are uncovered in earlier phases.

* * * * *

Conclusion

SIMA is pleased to have the opportunity to comment on the Discussion Paper. Please feel free to contact me by email at amitchell@sima-amvi.ca. I would be pleased to provide further information or answer questions you may have.

Yours sincerely,

THE SECURITIES AND INVESTMENT MANAGEMENT ASSOCIATION

By: Andy Mitchell
President and CEO

APPENDIX A

Responses to Questions Posed in CSA Multilateral Discussion Paper 11-406 – CSA Financial Innovation Hub Introduces Collaboratory and Data Portability Test

1. What changes have you made in your organization (or that you expect to implement) to comply with existing or forthcoming Data Portability obligations, and what challenges have you encountered?

   Response:

   a. For the implementation of Quebec data portability right, certain SIMA members found that changes were needed to: (i) policies and procedures; (ii) staff tools and training; (iii) data access protocols; and (iv) in some cases, updates to technology or systems. Challenges encountered were (i) limiting shared data to computerized personal information; (ii) excluding third party data and data that is created or inferred by the organization (i.e. investor risk rating); and (iii) communicating the information in a structured and commonly used technological format.

2. In what circumstances has there been a conclusion that the costs and complexities in implementing Data Portability resulted in the organization not being required to comply with such obligations? Are any of these related to securities legislation?

   Response:

   Below are insights from members involving the Quebec data portability right and the Federal Framework[4] on consumer-driven banking.

   a. **Quebec** – For the implementation of Quebec's data portability right, firms need to conduct a case-by-case analysis to determine whether "serious and practical difficulties" may preclude a firm from complying with an individual's request for data portability. If complying with a request entails particularly high costs or significant complexity, a firm may be able to justify rejecting the request. As Quebec's right to data portability came into force in September 2024, there is limited guidance establishing any threshold over which a request cannot be met. To date, no guidance has specifically identified a hurdle created by securities legislation that justifies rejecting a data portability request in Quebec.

   b. **Federal government** – For the Federal government's consumer-driven banking initiative, the application to investment accounts in a bank's related securities entities will require a gap analysis between the federal government regulations (once published) and any potential securities regulatory requirements. For example, whether costs and complexities and/or "serious and practical difficulties" are the basis for not complying with a data portability request. To date, there has not been an identification of a hurdle created by securities legislation in connection with the Federal Framework.

3. How do you anticipate that Data Portability will impact the investor experience, particularly in terms of reducing friction during transitions between service providers? If clients have already begun exercising their rights by utilizing these services, what has the feedback been so far?

   Response:

   a. Based on the limited experience with the Quebec data portablity right, SIMA members anticipate that data portability has potential benefits and risks for the investor experience.

      Potential benefits:

      - Enabling computerized personal information to be more efficiently sent to the client in a secure manner.
      - Improving efficiency by processing personal information requests digitally as compared to manually pulling the documents and sending them to the client.
      - Potentially allowing the account opening process, in future, to be more user friendly for advisors and clients if the client's computerized personal information from another financial institution

[4] https://www.canada.ca/en/department-finance/programs/financial-sector-policy/open-banking-implementation/2024-fall-economic-statement-canadas-complete-framework-consumer-driven-banking.html

could be incorporated into the client onboarding tool and with other digital tools, subject to changes to securities laws and related guidance.

Potential risks:

- There could potentially be data quality issues when the data is transposed digitally (e.g. IT or systems errors). To minimize these errors, data quality checks would be needed prior to information being sent to the client or other financial institution which could increase potential delays and involve additional resources.

4. What are the circumstances that you anticipate having to transfer data with external parties? How prevalent are these circumstances? Are there other regulatory obligations in securities legislation that market participants anticipate can be better satisfied through use of Data Portability?

   Response:

   a. For the purposes of this response, external parties exclude securities registrants.

   b. Depending on the scope of data portability framework, there could be new circumstances arising where securities registrants are requested to send or receive client data between non-securities registrants. For example, third-party data repositories where clients hold their information.

   c. Data portability may help support existing account transfer processes applicable to investment dealers (i.e. CIRO Rule 4800, Part B.1). However, careful coordination with existing service providers would be needed to determine if data portability could lead to challenges with the existing account transfer process.

5. What motivated you to consider adopting an e-KYC or other Data Portability solution and what features and improvements would you like to see in the future? Alternatively, if your organization would not consider adopting an e-KYC or Data Portability solution, what is the principal reason for not doing so?

   No response provided – firm specific question.

6. In what ways could e-KYC and Data Portability contribute to broader inclusion of investors? What steps can be taken to ensure that individuals who may have limited access to traditional identification systems are not disadvantaged by these innovations?

   No response provided – firm/service provider specific question.

7. Are you aware of other e-KYC or Data Portability business models being considered?

   No response provided – firm specific question.

8. What sorts of information do registrants anticipate transferring? What types of data would it be useful for registrants to obtain upon new client onboarding or at other times? Is there certain data that registrants have concerns with being required to transfer?

   Response:

   a. Transfer of client identification data is recommended at the outset. It is anticipated that this information may be useful to help initiate client onboarding and reduce potential friction of clients or advisors entering such information. Over time, increased optionality for data transfer may be considered (i.e. account holdings, personal and financial circumstances) as the fundamental aspects of the data portability and e-KYC solutions are advanced.

9. Are there circumstances in which transfer of data enhanced by other market participants to provide additional value, such as risk tolerance assessments, would be appropriate, and if so, what are those?

   Response:

   a. A potential circumstance could be transferring enhanced data, such as risk tolerance assessments, to assist the data recipient to understand the client's personal and financial circumstances to complete KYC and conduct suitability more efficiently.

b. Potential risks with sharing risk tolerance assessments are:

- inapplicability of the data to the account type to be opened at the data recipient;
- over-reliance by the data recipient on enhanced data without independent inquiry; and
- differences between the methodology of the data holder and data recipient in developing the specific enhanced data (i.e., the firms may use different methodologies in determining client's risk tolerance) that may diminish any value in sharing and subsequently using such enhanced data.

10. In your opinion, are there any provisions or requirements in securities legislation or guidance that may create barriers on how your organization can utilize e-KYC or Data Portability solutions? If so, in your view, what is the most appropriate regulatory action that would enable or assist your organization to utilize an e-KYC or Data Portability solution (e.g., specific rule change, additional guidance)?

Response:

a. Anticipated barriers in securities legislation or guidance may include:

- Requirements of securities registrants to conduct and update KYC[5] information and related due diligence, including a meaingful interaction with clients as well as suitability obligations[6].
- Prohibition on securities registrants delegating KYC[7] and suitability obligations[8].
- Existing CIRO guidance regarding KYC[9] including:
  - dealers and registered individuals should not pre-populate questionnaires with KYC information (other than biographical information which the dealer already has) 10; and
  - conditions when KYC may be used for multiple accounts11.
- Complaints by clients and/or regulatory compliance findings with respect to a data recipient if KYC information is incomplete, inacurate or not updated within securities regulatory timelines (i.e., 12 months for managed accounts and 36 months for non-managed accounts).

b. Regulatory action to address such barriers may include:

- Revising existing securities legislation and CIRO guidance regarding KYC collection to clarify practices for the use of KYC information received through data portability and e-KYC solutions.
- Addressing the extent and apportionment of liability and responsibility for data holders and data recipients with respect to regulatory investigations, audit findings and enforcement actions. This is to address concerns from securities registrants with potential liability and responsibility associated with participating in data portability and e-KYC solutions, and accordingly, are looking to securities regulators to help mitigate.

11. If you have already implemented an e-KYC solution, what specific challenges have you faced in implementing the solution? Have you faced challenges in implementing e- KYC or Data Portability solutions relating to varying regulatory frameworks internationally?

No response provided – firm specific question.

[5] National Instrument 31-103 *Registration Requirements, Exemptions and Ongoing Registrant Obligations* (NI 31-103), section 13.2.

[6] NI 31-103, section 13.3.

[7] Companion Policy to NI 31-103, section 13.2.

[8] Companion Policy to NI 31-103, section 13.3.

[9] CIRO Guidance on Know-your-client and Suitability Determination 21-0244 (GN 21-0244).

[10] GN 21-0244, section 2.12.

[11] GN 21-0244, section 2.7.

12. To what extent would industry-wide collaboration on Data Portability standards benefit registrants, and how can regulators such as the CSA support this collaborative effort? What challenges or barriers exist in developing and adopting such standards?

Response:

a. SIMA members support standardization of data portability standards, where applicable. Such collaboration should consider the core elements of the Federal Framework adapted to the securities industry, as appropriate, namely:

- the types of data and functionalities that are in scope for data portability along with the permitted participants, and the pace at which the system should expand;
- accreditation for entities seeking to receive client data from data holders;
- common rules;
- soundness of the securities industry;
- technical standards and technological barriers to implementation; and
- governance involving the oversight and management of the data portability framework.

13. How does a registrant ensure that investors are fully informed and able to provide meaningful consent for the use of e-KYC and other Data Portability solutions? What improvements could be made to better inform customers about their data ownership rights and portability options? What measures could be taken to enhance customer understanding and control over their data?

Response:

a. Based on an understanding of the Federal Framework, clients will need to be engaged by both the dataholder and the data recipient to facilitate the transmission of client data:

- Client authorization to share their data – client authorizing dataholder to share their data with the data recipient (the Authorization); and
- Client consent to collection and use of the data – client consenting to the use of the transferred data by the data recipient (the Consent).

b. At the time of seeking an Authorization or Consent, the data holder seeking the Authorization and the data recipient seeking the Consent, respectively each need to provide clients with sufficient information in a plain language, user-friendly information format.

c. The CSA, in collaboration with CIRO, should develop educational campaigns for dealers and advisers to better equip them to help clients navigate a data portability solution. In addition, clients should be informed about how they can revoke their Authorization and Consent. Collaboration with the Federal Consumer Agency of Canada is also encouraged given the potential harmonization of the Federal Framework.

d. Securities registrants will also need to consider updating existing privacy policies, procedures and disclosures to reflect data portability solutions. They may also want to develop training tools to help their staff answer client inquiries.

14. What risks arise from the use of e-KYC and other Data Portability solutions? What regulatory measures or industry best practices would be most effective in addressing those risks? How can the CSA help ensure that investors are protected while enabling innovation in this space?

Response:

Below are certain identified risks that may arise from data portability solutions. Potential mitigants and approaches have been included to help foster investor protection while mitigating the potential regulatory burden for securities registrants. However, further risks may arise depending on the participants involved and the scope of the data portability solutions.

Risk	Potential mitigants/approaches
Accuracy/completeness: risk that the client information shared by the data holder is incorrect or out of date. Also the data provided may be insufficient for the account type and/or products to be held with the data recipient so additonal information will still need to be collected from the client to complete KYC.	• Individuals are solely responsible for the accuracy of the data that they provide to securities registrants. Therefore, the Authorization must include an acknowledgement to this effect. • Securities registrants are not required to update or confirm the information stored for clients as part of a request to share data. Existing policies and procedures for engaging with clients that comply with securities legislation will continue to apply. • Data recipients continue to be responsible for collection of data from a client in order to complete KYC.
Cybersecurity/security: risk that the client data transmitted by the data holder at the request of the client is accessed by an unauthorized party.	• A single regulator to provide oversight and/or accreditation of any participants handling client data including data aggregators and data recipients. Criteria for accreditation may include security controls, policies, and incident response capabilities. • In consultation with key stakeholders, CSA to develop procedures and terms of agreement for data holders, data recipients and other parties involved in a data portablity solution. We refer the CSA to the Account Online Notification (ATON) system procedures[12] as an example.
Liability and responsibility for parties transmitting client data: attributing liability and responsibility in cases of errors or security breaches.	• CSA to address the extent and apportionment of liability and responsibility of data holders and data recipients in respect of regulatory investigations, audit findings and enforcement actions, and potential indemnities between participants. The assignment of liability and responsibility may apply in the event of errors in client data that is provided by the client which is outside of the data holder's control to verify or correct.
Negative user engagement: clients may encounter friction in the process of providing and revoking their Authorization and Consent for data portability.	• Data portability participants to develop a framework for collecting the Authorization and Consent that satisfies minimum requirements set by a single regulator to ensure a consistent client experience.
Service disruption risk: enhanced risk of service disruption if a registrant delegates data portability function to a third-party, non registrant.	• Consider the application and potential revision of existing guidance on outsourcing arrangements involving securities activities, such as CIRO guidance[13].
Supervisory risk: enhanced risk if a registrant delegates data portability function to a third-party, non-registrant.	• Consider the application and potential revision of existing guidance on outsourcing arrangements involving securities activities, such as CIRO guidance[14].

[12]ATON procedures https://www.cds.ca/resource/en/57

[13]CIRO, Guidance Note 2300-21-003 https://www.ciro.ca/newsroom/publications/outsourcing-arrangements-0

[14] CIRO, Guidance Note 2300-21-003 https://www.ciro.ca/newsroom/publications/outsourcing-arrangements-0

15. Do you see any security or accuracy issues arising with respect to utilizing an e-KYC or other Data Portability solutions for a large number of clients?

Response:

a. SIMA notes potential security and accuracy issues associated with utilizing data portability solutions for a large number of clients, whether the use is client-initiated or registrant led.

- Client-initiated use: the use of data portability solutions for a large number of clients could increase the potential risks noted in our response to Question 14 above.
- Registrant-led use: data portability may be considered by securities registrants to facilitate a bulk movement of client information. As background, client account transfers involving a large number of clients could occur with or without prior client authorization. For example, a large number of clients can authorize the transfer of their accounts when their investment adviser moves from one dealer to another dealer. Alternatively, no client authorization is required if exemptive relief is granted from CIRO for a bulk transfer of accounts. CIRO has developed rules on account transfers and bulk account movements between CIRO dealer members. Please see CIRO Rule 480015, including Rule 4866 regarding exemptions for bulk transfers.

16. How do current industry standard KYC processes mitigate risks such as deepfakes, synthetic identities, identity fraud, and regulatory non-compliance, and what additional measures or technologies could be implemented to enhance protection against these threats?

Response:

SIMA recommends that this topic be raised as a separate regulatory consultation.

17. What technological infrastructure is required to support efficient Data Portability, and how does the cost of implementation impact your business? Are there specific technologies or innovations that could help reduce costs while maintaining security and compliance?

Response:

a. Consistent with and to the extent applicable to securities registrants, it is recommended that the CSA align to the Federal Framework and provincial regulatory initiatives, such as the Quebec data portability legislation, to foster harmonization and minimize costs.

b. Commentary on costs requires a framework and use cases for data portability. As a result, cost estimates cannot be provided at this time.

18. How do third-party service providers (e.g., data aggregators, e-KYC platforms) influence the Data Portability process? What role should these third parties play in facilitating secure and compliant data transfers, and what regulatory oversight might be necessary?

Response:

a. Third-party service providers play a critical role in the data portability ecosystem. Consistent with the treatment of clearing agencies, we recommend that the CSA consider oversight and/or accreditation of third-party service providers engaged in the data portability ecosystem. Such oversight and/or accreditation may need to be coordinated with the federal Financial Consumer Agency of Canada in connection with consumer-driven banking.

b. CSA recognition and oversight will help promote safety and soundness of the data portability ecosystem and instil confidence in such processes by clients and industry participants.

[15] CIRO Rule 4800 https://www.ciro.ca/media/16/download?inline

19. How do you foresee blockchain or AI impacting the implementation of data portability and e-KYC? What steps can regulators take to prepare for these technological advancements while maintaining market integrity?

Response:

a. **Blockchain:** Blockchain technology effectively functions as public ledger. The benefit of using blockchain in the context of a data portability solution is that it will form a record of how, and to whom, the data has been transferred. However, one of the core issues with using blockchain technology is its lack of scalability for data transfers. It would be challenging to scale this technology to the extent that would be required for use in frameworks like consumer-driven banking. A SIMA member noted that to the best of their knowledge blockchain is currently not contemplated as being a fundamental requirement for the federal consumer-driven banking framework. If an opportunity arises to develop a platform that would allow for the use of blockchain for data portability (either by government bodies or regulators), SIMA recommends that securities regulators ensure that the platform is built according to common or previously established international standards. Creating new or different standards could result in redundancies and would undermine the objective of these initiatives.

b. **AI:** SIMA recommends a similar approach to the use of AI in data portability by securities regulators as in blockchain, in terms of ensuring that the platform is built according to common or previously established international standards. Securities regulators need to ensure that they are following and co-ordinating with internationally recognized standards for the use of AI. A coordinated and uniform approach is essential to the success of initiatives like data portability.

20. Data Portability often involves the transfer of customer data across jurisdictions. What regulatory or operational challenges do you encounter when facilitating cross-border data transfers, and how can regulatory frameworks better support such transfers in a compliant and secure manner?

Response:

a. SIMA seeks clarity regarding the meaning of “transfer” of customer data. Does this refer to the transfer across Canadian jurisdictions and/or internationally? Does it refer to data centres where data may be stored?

b. Potential regulatory or operational challenges include:

- client consent and/or authorization to permit cross-border data transfers; and
- differing privacy and data protection standards in jurisdictions where data transfer may occur which could lead to impairment of client rights.

c. SIMA recommends that the scope of cross-border data transfers is limited to jurisdictions with requirements that are reasonably designed to achieve investor protection and help minimize risk to securities registrants participating in data portability.

21. To what extent would standardized data formats (such as those proposed by the consumer-driven banking framework) facilitate Data Portability between registrants? Are there existing frameworks or standards that should be adopted or modified to improve interoperability? Are there risks or disadvantages to such standardization?

Response:

a. As a guiding principle, SIMA supports harmonization when developing standards for data portability. However, clarification is sought regarding the term “data format”. For example, whether the reference to “data format” refers to the method of transmitting client data (i.e. API), the specific data elements (i.e. client name, address) to be transmitted or another reference.

22. Would you be interested in participating in either the Phase 2: Industry Consultation Forum or Phase 3: Live Testing Environment? If you are interested in participating in the live testing environment, how do you think you will be able to participate? (e.g., as a registrant using potential e-KYC services, or a potential e-KYC service provider)?

    No response provided – firm specific question.

23. Although this first theme deals with emerging issues related to data portability and e- KYC, CSA staff are interested in developing further cohort-based testing environments. To that end, we are interested in understanding if there are emerging areas for the CSA to consider in subsequent cohorts. Please let us know if there are any particular areas of interest for us to further consider in future Testing Environments.

    Response:

    SIMA recommends account transfers as a topic for future Testing Environments.

APPENDIX B

Test Overview

Figure 1 Examples of e-KYC portability Example

Example 1: a potential e-KYC solution provider

A live testing e-KYC environment could involve the following participants:

a. **An e-KYC portability service provider** that collects and holds client personal information, who is then authorized or directed by the client to release some or all of that personal information to registrants periodically in order to facilitate processes of the registrant, such as account opening or annual maintenance.

b. **Clients** who are interested in utilizing an e-KYC portability service provider to streamline account opening and to periodically check for updates. These clients may find a benefit from reduced friction in the KYC process, particularly if the client is considering a number of different unique investment products that are only available from certain registrants.

c. **Registrants** that become part of a network of organizations that have partnered with one or more e-KYC portability service providers.

Example 2: direction by client to release KYC information to another registrant

Another example is a circumstance where:

a. **a client** has an existing relationship with an **investment dealer** (existing registrant). They wish to maintain the relationship with the existing registrant but also wants to invest in a product only available with an exempt market dealer, such as a **crowdfunding portal** (crowdfunding portal).

b. Instead of undergoing the standard onboarding process with the crowdfunding portal and completing all of its standard intake forms, the client directs and gives their consent to the existing registrant to release certain KYC information currently held by the existing registrant to the crowdfunding portal directly.

In both examples, the information is collected by the receiving registrant, who then reviews the information to determine what additional information is needed from the client to fulfill its KYC obligation. Once the information gap is determined, the receiving registrant engages in a meaningful interaction with the client to obtain the additional information. The receiving registrant will then be in a position to provide its suitability assessment.

Please note that these are only two potential applications of e-KYC portability, and that in addition to existing applications, other applications may be developed over time.