IIACACCVM
INVESTMENT INDUSTRY ASSOCIATION OF CANADA
ASSOCIATION CANADIENNE DU COMMERCE DES VALEURS MOBILIÈRES

701 West Georgia Street | Suite 1500
Vancouver, BC | V7Y 1C6
604.637.1677 | www.iiac.ca

www.iiac.ca

Susan Copland, LLB, BComm
Managing Director
scopland@iiac.ca

September 23, 2020

Direction du Secrétariat des commissions
Assemblée nationale du Québec
Édifice Pamphile-Le May, 3e étage
1035, rue des Parlementaires
Québec (Québec) G1A 1A3

Dear Sir/Madam:

Re: Québec Bill 64 – *An Act to modernize legislative provisions as regards the protection of personal information* (the "Bill" or the "Proposals")

The Investment Industry Association of Canada (the "IIAC" or the "Association") appreciates the opportunity to comment on the Bill. The IIAC is the national association representing 114 investment dealer firms on securities regulation and public policy. Our members are the key intermediaries in Canadian capital markets, accounting for the vast majority of financial advisory services for individual investors, and securities trading and underwriting in public and private markets for governments and corporations.

IIAC members provide financial advisory services to millions of Canadians, collectively holding 6,615,000 Full-Service Brokerage Accounts, as well as many other self-directed, digital, and hybrid accounts. In servicing these accounts, our industry is responsible for safeguarding some of our clients' most personal information, including the details of and access to their accounts and financial data.

The effect of the ongoing digital revolution has, and will continue to have an enormous impact on individuals' daily life and the operation of virtually every business. The regulation of data use has far-reaching implications into the way in which business is conducted. Regulation impacts foundational business decisions, including whether the cost of serving clients in a meaningful and personalized manner is feasible, given the regulatory structures that may be set up to protect their data. Therefore, it is critical that proposed regulation be structured to account for the way in which different industries use technology and data, allowing for best practices among such industries to develop, rather than imposing a one-size-fits-all approach to all industries.

We are deeply concerned that the Bill contains a number of provisions that are not only inconsistent with other domestic and international privacy regulations, but are also extremely burdensome, virtually impossible to operationalize, and do not provide individuals with meaningful protection of their data.

A foundational premise of the *Personal Information Protection and Electronic Documents Act* ("PIPEDA"), is the recognition of the need to balance individuals' privacy rights with business needs for the use of data, in order to encourage the development of the digital economy and technological solutions that are critical to creating a strong and competitive economy. Unlike PIPEDA and the *European General Data Protection Regulation* ("GDPR"), the Bill does not articulate a similar foundational objective.

We urge the Québec Government to work with the Department of Innovation, Science and Economic Development Canada ("ISED") and the relevant provincial regulators in British Columbia, Alberta, and Ontario to develop a harmonized privacy regulatory framework applicable across Canada. Currently, the provincial and federal privacy laws are relatively consistent in terms of content and results. Introducing inconsistencies increases uncertainty, creates inefficiencies, and increases the cost of compliance for Canadian entities operating within Canada, and foreign entities seeking to do business in Canada. A harmonized approach also facilitates a simplified interface with the GDPR and other international regulatory regimes that recognize the regulatory approach of other jurisdictions in respect of compliance with their own regulation.

In particular, there are a number of areas of the Bill that are of significant concern to our industry.

Accountability

The current Québec *Act respecting the protection of personal information in the private sector* departs from PIPEDA, in that it is not underpinned by the principle of accountability by the companies subject to it. Although the Bill introduces a number of provisions that require firms to implement specific privacy governance measures, it does not provide firms with sufficient flexibility to implement policy and procedural safeguards that are appropriate to their particular operations, and make firms ultimately responsible for ensuring that those measures achieve their objectives.

As noted above, one way to create accountability is to facilitate the creation of specific industry best practices, taking into account the way the industry collects and uses data, overseen by industry regulators where appropriate.

Policies and practices

In attempting to provide transparency, and ensure some accountability, the Bill requires that enterprises in Québec establish, implement, and publish governance policies and practices regarding the protection of personal information. These policies must be very in-depth and detailed in order to deal with internal personnel and processes. While it may be appropriate for firms to develop detailed internal policies for dealing with data, it is inappropriate for firms to be required to publish these policies and processes. Although it is general practice for organizations to publish privacy policies and notices on their website pursuant to transparency requirements set out in PIPEDA, publication of detailed internal privacy policies and procedures is not general practice, and does not provide useful information to the public, due to the

length and complexity of such disclosure. In addition, policies may contain information upon which some companies compete, making them further unsuited for publication.

Consent

We are extremely concerned with the proposed requirements for enhanced consent under the Bill, particularly in respect of data processors and transborder transfers of data. We expressed our concerns relating to a similar proposal advanced by the Canadian Office of the Privacy Commissioner (the "OPC") in 2019. Upon receiving significant feedback, the OPC withdrew the proposal, acknowledging the difficulties posed by obtaining specific consent prior to collecting, using or disclosing individuals' personal information. On August 4, 2020, the OPC issued the PIPEDA Report of Findings #2020-001, affirming that specific consent is not required for transborder processing of data.

Given the vast amount of data that is collected and used in increasingly novel and unanticipated ways as technology evolves, the principle of obtaining specific and detailed consent for each use of data that may be involved in the provision of a product or service, is unworkable and ineffective, and would be virtually impossible to operationalize.

Rather than requiring specific consent, we believe that it is more appropriate to rely on the principle of accountability, both for the entity for which the data is being acquired and used, and entities that are used by that entity for processing the data. These principles underpin the federal PIPEDA legislation, negating the need for specific consent for transfers for processing purposes only, and for transborder data flows. It is more appropriate to create a consent exemption that relates to standard business practices for the provision of the services for which the client has contracted. This framework for client data protection is consistent with the reasonable expectations of clients.

The proposed consent requirements would introduce an element of regulatory misalignment with provincial, and other international privacy regulations, and overlay the Canadian accountability regime with a consent regime. While there is some similarity with the GDPR's consent requirements, it should be noted that the GDPR's consent requirements are only required in narrow circumstances, and include several legal grounds for processing, including legitimate business interests, which the Bill does not clearly exempt. This inconsistency makes the Proposals considerably more burdensome than PIPEDA, British Columbia Personal Information Privacy Act ("PIPA"), Alberta PIPA, and the GDPR.

We are particularly concerned with the provision that consent must be given for each specific purpose, separately from any other information provided to the person concerned. In a data-driven industry, providing services requires that information is processed in many different ways by many different processors, and technology is continually evolving so that new applications are continually introduced to enhance service. In this context, clients would be faced with overwhelming ongoing requirements to repeatedly consent to a litany of data use applications for many processors required by members in order to deliver quality service. This places an unrealistic burden on the client to read, understand and sign off on lengthy and sometimes complex privacy policies that will necessarily vary between firms and industries.

This may also provide an opportunity for cyber criminals to use the proliferation of consent requests to plant malware and perpetrate cyber-crime. This has occurred in Europe, where cyber criminals have used provisions in the GDPR to overwhelm data custodians with demands for disclosure of personal data.

Effect on the investment industry

The investment industry manages a vast amount of data, including information related to banking, assets, liabilities, and taxes; personal identification information and details about family members; and other information required to facilitate financial planning and provide investment management services to clients. In order to provide services to investors, many third-party processors are involved in the investment process, as data is aggregated, disaggregated, analyzed, categorized, manipulated and stored in order to undertake and complete the many steps in the investment, trading, settling, clearing, reporting, and compliance functions.

In order to protect this critical data, investment dealer firms have developed robust data protection processes and safeguards within their firms, and in their interaction with third-party processors. The industry has also worked closely with its regulator, the Investment Industry Regulatory Organization of Canada ("IIROC") to ensure clients benefit from appropriate protection of their data.

Significant changes to the established processes for managing the protection of client data would have an adverse effect on the ability of dealer firms to provide such services, which in turn would affect clients' ability to access financial services from their preferred firm, if at all.

Currently in Canada, there are 6.6 million full-service accounts. Consent is obtained at the point of onboarding to cover all anticipated purposes and uses of client information during the servicing relationship. New data use purposes that were not contemplated at the onboarding stage do require additional consent under PIPEDA, but typically the initial onboarding consent is comprehensive enough that additional consents are rarely required. For firms, the process of ongoing notification and obtaining of additional consents for a "new specific processor" (as opposed to the "action of processing", which remains the same), providing for opt-outs where applicable, and tracking, would be virtually impossible to implement and enact on an ongoing basis.

Requiring new disclosure and consent for these existing accounts would require re-papering the accounts for consent, which is not only impractical, but would likely result in interruption or delay of service for the many clients that may ignore the barrage of consent requests resulting from the Proposals. The results could potentially be very detrimental for clients, as timing can often be critical in dealing in the financial markets.

We believe the Proposals do not strike an appropriate balance between affording additional investor protection and imposing a significant burden on firms and clients.

Investors have a reasonable expectation that investment firms will have appropriate security processes in place, and will ensure that the third parties they deal with will also protect their clients' data. Requiring clients to expressly consent to the transfer of data for processing will not provide additional protection, as the ultimate choice for the consumer becomes either to trust the investment firm and receive the services or terminate the agreement.

A practical and effective approach is to ensure there are consent exemptions for the standard business practices needed to deliver the services clients expect when they contract for the service, and accountability of the firm and the processors where issues arise.

Rather than requiring a more stringent consent regime, we recommend that the focus be on disclosure, i.e. that organizations provide plain-language disclosure stating how they will use client data in respect of carrying out their business activities.

We believe that a model where firms provide reasonable disclosure and are ultimately held accountable for the use of client information—consistent with the approach taken under PIPEDA, is a more effective means of ensuring that the use of personal information is appropriate and consistent with client expectations. The accountability principle in PIPEDA is a key driver of privacy compliance by organizations. Requiring additional consents from individual clients does not advance the fundamental objective of protection of client data or give clients additional options for data handling. Where clients provide additional express consent, it may, in fact, shift some responsibility onto clients, which could erode the concept of accountability for data, that is currently at the heart of the Canadian privacy regime, and that of the GDPR. It could also arguably shift the user's accountability to the "consenting" client, and mitigate available damages should an issue arise as a result of the transfer of data. Any resulting diminution of accountability or mitigation of damages works against consumer interests, contrary to the objective and philosophy of the regulation contained in the Bill.

We agree, however, that obtaining specific consent is important to ensure transparency and accountability where individual data is to be used in a manner that is not integral to the provision of services for which the individual has contracted, for example, where data is being provided to third parties that are not involved in the provision of such services.

In respect of transborder data flows, the consent requirement would be unworkable. Many processing functions, notably cloud computing, occur in non-Canadian jurisdictions. The requirements for transborder flows should not differ from other processing activities and should be underpinned by general disclosure and accountability. The fact that a transaction within Canada itself (i.e. from one province to another) is considered "transborder", is particularly problematic and unnecessary, given the strong and consistent Canadian regulatory regime.

Also problematic is that the Bill indicates that if the legislation in the other jurisdiction is not considered of the "same degree of equivalency", then the transfer of information is prohibited, and cannot be conducted, even if the client consents to the transfer.

We are also extremely concerned that the firms must conduct their own assessment of the adequacy of the privacy regime in other jurisdictions. This too would be unworkable, as firms would not have the expertise and resources needed to evaluate the equivalency of other jurisdictions' privacy regime. Further, there is significant risk of inconsistent evaluation of such regimes by different entities.

No employee consent exception

We note that the Proposals do not include an employee consent exception. Under PIPEDA, British Columbia PIPA, and Alberta PIPA, employers can collect, use and disclose personal information that is necessary for establishing, managing or terminating an employment relationship, without the consent of their employees, although they have a duty to inform employees of their practices.

Sensitive personal information

We do not believe "sensitive personal information" should be defined, as it is likely to be contextual, based on other information collected at that time or later. Defining "sensitive personal information" and adding additional protections would increase the burden without providing additional meaningful protections, particularly where this information is required in order to deliver the desired service and is consistent with the reasonable expectations of the client. Again, the concept of accountability should be relied upon to ensure data security.

Mandatory privacy impact assessments

We are concerned that the requirement that enterprises conduct an "assessment of the privacy-related factors" with respect to any "information system project" or "electronic service delivery project" involving the processing of personal information is overly broad and is not subject to a materiality threshold, unlike the provisions in the GDPR Article 35(1), which only require a privacy impact assessment where the processing "is likely to result in a high risk to the rights and freedoms of natural persons".

Privacy by design

We agree that it is appropriate that enterprises collecting personal information through technological goods or services follow a "privacy by design" approach. However, the standard set in the Proposals, requiring that firms' technological products or services provide the "highest level of confidentiality by default, without any intervention by the person concerned", is extremely problematic. This standard does not take into account the risk profile of the system, information, or technology, thus imposing potentially prohibitively expensive data protection measures on all systems, without regard to the function of such systems.

This approach is also inconsistent with the GDPR, which expressly takes into account the circumstances surrounding a particular initiative, including the costs of implementation and degree of risk for individuals involved.

We are also concerned that the standard of "highest level of confidentiality" is a new construct not used elsewhere in the privacy arena to-date, and that proposed Section 9.1 does not provide any indication of what would be considered the "highest level of confidentiality" in a given context. We recommend that a reasonability standard, referring to reasonable commercial considerations and business models, be introduced into this provision.

Breach notification requirements

We support the introduction of new breach notification requirements into the Proposals. However, it is critical that the requirements be consistent with PIPEDA and other relevant privacy regulations, in order to ensure that enterprises are not subject to different triggers, thresholds, and requirements, for the same incident, during a time when the entity would be focused on containing and mitigating the damage that may have resulted from the breach. We recommend that the threshold of a "confidentiality incident" that presents a "risk of serious injury" to the individual, be amended to be consistent with the "real risk of significant harm" as defined under PIPEDA.

Obligation to inform individuals of the use of a technology that allows them to be identified, located, or profiled

The investment industry is characterized by the use of analytics that tailor beneficial financial products and services to individuals, based on their profile. The ability of the industry to provide these important services to their clients would be seriously undermined by the provisions in the Bill.

While it is reasonable for firms to generally inform their clients that they are using technology that could allow an individual to be identified, located, or profiled, it is wholly impractical for the firm to identify each processing activity that may effectively create or use these profiles. It is also impossible to provide services if firms are required to deactivate the functions that allow them to do so.

Data portability

The IIAC has some questions and concerns in respect of the proposal to provide an explicit right for individuals to direct their personal information be moved from one organization to another in a standardized digital format. We support the principle of data mobility as a means to assist individuals in controlling their data, and as an efficient means for companies to manage consumer information. However, the data subject to these provisions must be clearly and narrowly defined in order to be operationally feasible, and to prevent confusion and inappropriate disclosure. For instance, the process for one organization to move a defined subset of the information they hold to another organization (where not all of the consumer information would be relevant or appropriate for them to possess) should be straightforward.

A possible unintended effect of data mobility that is not confined to specific and required information could be to multiply the number of databases containing information about individuals, rather than limiting them. This would occur as firms tried to ensure that they limited certain types of information that could be subject to data mobility requests.

We recommend that the categories of data that will be subject to mobility be clearly defined, so that only the appropriate and relevant data can be transferred between organizations. We agree with the proposal that the data should only include information provided by the individual, and not derived or third-party information.

The data mobility provisions should also be contingent on organizations having appropriate technical standards covering data compatibility, authentication, security, and other relevant controls. The timeline to mandate data mobility must take into consideration the time required to develop industry standards.

From a practical standpoint, the data subject to mobility requirements should be differentiated by industry. For instance, individual data provided to financial firms should only be sharable amongst other financial firms, and not, for instance, with health care providers. By categorizing the data, and limiting its mobility in this manner, the likelihood of data leakage is minimized. In addition, the appropriate data sets, standards and formats would be more easily standardized within industry categories, as similar programs and protocols already exist to allow organizations to communicate and share data with each other. It is impractical to impose similar technology standards, protocols and formats across industries where data is collected, stored and used in very different ways and for very different purposes.

Right to be forgotten

While we agree that individuals should have some measure of control over their data once its purpose has been achieved, we are concerned that the Proposals introduce significant operational burdens for industries that use data in a variety of functions, in different departments of the same organization, or use processors to provide services.

For instance, the investment industry collects a significant amount of data about its clients, in order to provide high-value investment, financial planning, and trading services, targeted specifically to client circumstances. This information is not made public, and is used/shared only within/between the firm and the third-party processors required to provide the contracted services.

It should also be noted that the self-regulatory rules governing investment professionals have prescriptive retention and deletion policies that were developed to specifically address the way in which the industry operates, and the expectations of clients. The Proposals would introduce prescriptive measures that could conflict with certain existing industry provisions, and create significant compliance challenges in respect of data that is used in different ways within the firm, and shared with various processors in order to deliver a variety of services to the client (e.g., trading, financial planning, tax planning, retirement savings).

We recommend the Proposals be targeted to organizations and platforms that provide online public access to information about individuals, rather than for the provisions to apply to businesses that do not have an impact on an individual's online reputation.

Right to object to automated processing

The right to object to automated processing, articulated in Section 12.1 of the Bill, is wholly unrealistic and out-of-step with the established use of technology to provide high-value, targeted services, which is only possible through the use of data analytics.

In order to provide insights into the most appropriate products, services, and the manner in which to serve clients, it is standard practice for investment dealers to use automated processing of personal information to make a decision about an individual, in order to determine what product or service is optimal, based on an assessment of the individual's personal financial situation.

While it is possible and appropriate to provide individuals with general information about such processing, the prevalence and complexity of the analytics would make it impossible to provide individuals with specific information about all of the factors and parameters leading to the automated decisions.

It is appropriate to provide individuals the opportunity "to submit observations to a member of the personnel of the organization who is in a position to review the decision made by automated means", should the client believe that there is a material error in their personal information that is leading to problematic outcomes.

Administrative Monetary Penalties

We are extremely concerned with the inclusion of, and the potential quantum of the Administrative Monetary Penalties (AMPs). Given the complexity of the regulation, the multiple elements of the Bill that could lead to fines, the different uses of information by various industries, and the nuances in how industries use information, along with the broad range of contravention, it would be virtually impossible to administer and apply the penalty system in a fair and consistent manner. Given the size of the potential penalties, the impact of these penalties would have a significant chilling effect on the use and development of technology that could enhance services for consumers. The potential AMPs are also inconsistent with – and significantly larger than – the penalties under PIPEDA and other Canadian privacy regulations.

Penal regime

We are concerned about the extremely significant fines that could be levied under the Bill, and the fact that it would apply to more offences than the AMPs. As noted above, we are concerned about the chilling effect on the development of technology that would benefit industries, clients, and the economy in general. The potential penalties are also inconsistent with – and significantly larger than – penalties levied under PIPEDA and other Canadian privacy regulations.

Private right of action

We do not believe the private right of action is necessary, given the existing privacy provisions of the Civil Code of Québec that allow individuals to bring privacy actions before Québec court in cases of privacy violations. The addition of a private right of action could encourage class actions where no real damage has occurred.

Self-regulation and technical standards

The IIAC notes that, unlike the GDPR and the ISED proposals for PIPEDA, the Bill does not accommodate the use of specific industry-based codes, standards, and certification schemes. The development and reliance on industry-based codes would be extremely useful in improving regulatory agility and supporting responsible innovation. They also provide a measure of consistency and predictability in dealing with other jurisdictions, who look to these standards as assurances that organizations can conduct cross-

jurisdictional business (such as with GDPR jurisdictions) without the imposition of additional requirements.

Given the differences in size, operations, and use of data in different organizations, it is critical that the codes, standards and certifications are not developed as a "one-size-fits-all" model. Rather, they should be flexible to accommodate the specific data stored at an organization and the way in which data is used in that organization. It is important that, in order to be relevant and operationally practical, the industries that would be using these codes, standards and certification schemes be involved in the development of the protocols and standards.

The codes and certifications should not be mandatory but voluntary, as they may not be applicable or practical for all organizations to enact. Compliance with such codes would be evidence of firms' enactment of appropriate standards, and would be considered in the assessment of liability if clients' information is compromised. In this way, all firms, particularly those handling a higher volume of personal information would be incentivized to comply with the relevant codes.

We believe the codes and certifications should be administered by a third-party certification body, which is accredited by the Standards Council of Canada, and overseen by the appropriate industry regulator (such as IIROC), where appropriate. This would ensure that the industry regulator applies the codes in the proper context, as they would have knowledge of the way in which data is used and protected in that specific industry.

We also recommend that the use of such codes and certifications be recognized in the Bill, such that compliance would be taken into account in ascertaining appropriate remedies should a non-compliance incident occur.

Thank you for considering our comments. We would be pleased to meet with you, and other appropriate individuals responsible for developing the Proposals, to provide further input on the key considerations in data regulation for the financial industry. If you have any questions, please do not hesitate to contact me.

Thank you for considering our comments.

Yours sincerely,

Susan Copland