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

August 6, 2019

Office of the Privacy Commissioner of Canada
OPC-CPVPconsult2@priv.gc.ca

Dear Sir/Madam:

Re: Consultation on transborder dataflows (the "Consultation")

The Investment Industry Association of Canada ("IIAC or the Association") appreciates the ability to comment on the Consultation first published on April 9, 2019, clarified on April 23, and reframed on June 11, 2019, and the specific proposed consent requirements contained therein (the" Proposals"). Our letter is structured to address the April 9 and 23 consultation papers in the comments below, with our comments generally addressing the questions posed in the April 23 document rather than answering each specific question. The questions posed in the June 11 document are specifically addressed at the end of this letter.

The IIAC is the national association representing 118 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 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 IIAC strongly believes the Proposals will impose a significant burden on both firms and clients that will not afford additional investor protection. In addition, the enhanced consent requirement will detract from PIPEDA's stated goal to support and "promote electronic commerce", in that the costly and unwieldy regulatory burden created from its implementation will discourage innovative uses of personal data. We believe that relying on the principle of Accountability, rather than requiring specific consent is appropriate where the transborder data flows and transfers for processing relate to standard business practices relating to 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 digitalization of the investment industry has encompassed all aspects of the provision of services to clients, from the opening of an account, to asset allocation, trading securities, monitoring portfolio performance, financial planning and ensuring personal client contact takes place at key points in time. This digitalization has enhanced the client experience, allowing investors to benefit from the vast amount of information and analytical capacity designed to leverage the skills of their advisors. This provides investors with better results and increased access and control over the information they receive, enabling them to better understand and direct their financial decisions.

Investment dealers take their responsibilities for safeguarding this data very seriously. Firms have developed robust data protection processes and safeguards within their firms, and in their interaction with third party processors. The Investment Industry Regulatory Organization of Canada ("IIROC") has focused significant attention on its members' data protection practices, by issuing guidelines, conducting cybersecurity testing and undertaking detailed firm surveys and assessments in order to ensure clients benefit from appropriate protection of their data.

In addition to data protection regulations and guidelines imposed by industry regulators, our members are also subject to various provincial privacy regulations. Currently, the regulatory infrastructure to which are members are subject is relatively consistent across jurisdictions. The Proposals, however, would introduce an element of regulatory misalignment with provincial, and other international privacy regulations. The Proposals are inconsistent with the interpretations of the provincial regulatory regimes, and do not align with the European General Data Protection Regulation ("GDPR"). The Proposals overlay the Canadian accountability regime with a consent regime, whereas the GDPR's consent requirements are only required in narrow circumstances, in that the GDPR allows for several legal grounds for processing, including legitimate business interests, which the Proposals do not clearly exempt. This inconsistency makes the Proposals considerably more burdensome than GDPR.

The degree to which clients' personal information is subject to safeguards involves a balance between the risks inherent in processing the data, whether for trading and accounts, running analytics to track and optimize performance, providing the background for financial and estate planning and the benefits to clients of having access to these services at a reasonable cost, or at all. Large scale data storage and processing undertaken by firms is critical in managing and minimizing the costs of providing services to clients, ensuring that investment services are available to small and large investors alike at a cost they can afford.

We believe the Proposals do not strike an appropriate balance, with the consent provisions not affording additional investor protection, while imposing a significant burden on firms and clients.

Given the vast amount of data, including personal identification, information related to banking, assets, liabilities, taxes, details about family members and other information to facilitate financial planning, required to provide investment management services to clients, changes to the established processes for managing the protection of the data will have a significant adverse effect on the ability of firms to provide such services, which in turn affects clients' ability to access services from their preferred firm, if at all.

OPC Consultation Process

The Proposals represent an adverse material change, not only to how firms deal with transborder data flows, but with any information processing that is not carried out in-house.

As such, the consultation process for the proposed changes has been very problematic. Given the significance of the changes to the industry and its clients in terms of the cost and availability of key services, and the fact that the Proposals represent a complete reversal of established guidance that has been in place for 10 years, the process undertaken by the OPC to implement the Proposals is at odds with established practice, fairness, and past process of regulatory development involving robust and well considered industry consultation.

Rather than undertaking a comprehensive consultation process, the basis for the reversal appears to initially have been a post facto application of the proposed changes supported by certain elements of the Equifax decision, which was based on a number of other factors other than the need for enhanced consent for cross border processing.

Although the June 11, 2019 reframed discussion document indicates that during the re-examination period and until the conclusion of the consultation, the OPC does not expect organizations to change their practices, there still exists significant uncertainty, given the expressed intention of the OPC to amend its guidelines.

Given the significant consequences of the Proposals, including the consistency issues relating to provincial regulation, not only should such changes not be implemented through Guidance, they should be subject to the process required for statutory reform to the underlying PIPEDA legislation. The process should involve significant consultation with affected industries on a sectoral basis, including written submissions and in-person meetings. The comment period should also allow for respondents to fully ascertain and explain the impact of the Proposals, individually, and in respect of their sector.

Legislative Objective and Consumer Impact

Aside from the issues related to the regulatory process, we do not believe that requiring client consent for data processing, and specifically cross border processing effectively achieves the objective of the legislation, which in its title indicates is an "Act to support and *promote electronic commerce* by *protecting personal information*…." .

Specifically, we believe the consent requirement will have no impact on the security standards and data protection measures established by organizations that hold individuals' personal information. The accountability principle, which underpins PIPEDA, is effective to ensure the appropriate security is employed, and enforced by relevant regulators.

As noted above, the investment industry collects significant sensitive personal data in furtherance of its role to manage clients' financial affairs to achieve their personal objectives. This information is collected in the context of a highly regulated environment that is very data driven.

In order to achieve the clients' financial goals, it is necessary for the investment firms to work with other industry participants to store, process, analyze and provide reports using certain elements of client data.

These activities are an integral part of providing the service to clients, making it impossible for clients to receive the service without providing consent for the use of their data. The standard business process of outsourcing aspects of services is disclosed to clients and is therefore well understood by clients availing themselves of those services. Requiring additional consent in these circumstances is contrary to the *Principles Set Out in the National Standard of Canada Entitled Model Code for the Protection of Personal Information*, where section 4.3.3 states that "An organization shall not, as a condition of the supply of a product or service require an individual to consent to the collection, use or disclosure of information beyond that required to fulfil the explicitly specified and legitimate purposes". Currently, clients are also informed at account opening, and firms disclose on their websites how and why the firm will use clients' personal data, and that it may be processed in a foreign country and may be accessible to law enforcement and national security authorities of that jurisdiction.

The long-standing interpretation that a transfer of data is a "use" not a "disclosure" is appropriate, and represents a practical and reasonable position. Where information is collected for processing, only to be used for the purposes for which it was originally collected, there should be no additional requirement for consent, as clients would have already implicitly or explicitly provided that consent when contracting for services. Further, it is contrary to principles of fairness and natural justice that the OPC, without any legislative amendment, would contemplate a complete reversal of its clear guidance relied on by firms since 2009, based only on a recharacterization of the same standard business process as a "disclosure" versus a "use" of personal information.

Given that firms are accountable for the use of client information, requiring additional consents does not advance the 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 of the responsibility to clients, which could erode the concept of accountability for data that is currently at the heart of our privacy regime, and also that of the GDPR. It could also arguably enhance the user's deniability and mitigate available damages should an issue arise as a result of the transfer of data. If the diminution of accountability and mitigation of damages result, that works against the consumer interests, contrary to the objective and philosophy of the regulation.

The transfer of client data to processors, both domestically and internationally is a consistent practice among dealers. Clients seeking to opt out of such data transfer, will as a result, be opting out of the services. The requirement for further consent, therefore, would not be meaningful and would be contrary to clients' wishes. As noted, clients are advised of the use of their information upon account opening. Requiring enhanced consent for initial and ongoing processing will result in voluminous disclosure and consent requirements upon account opening, as well as ongoing requirements for consent. Any ongoing enhanced consent requirements would lead to delays in trading and processing, where consent is not provided on a timely basis, ultimately prejudicing clients. It would also potentially lead to a deluge of consent requests, not only from investment firms, but the other many organizations that gather and use client information and have it processed domestically and internationally.

The amount of express consent requests and accompanying disclosure is likely to be overwhelming and annoying for individuals, who may ignore these requests for consent to their detriment. It may also provide an opportunity for cyber criminals to use the proliferation of consent requests to plant malware and perpetrate cyber-crime.

Investors have a reasonable expectation that investment firms will have appropriate security processes, and will ensure the third parties that 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 effective choice is to trust the provider and receive the services, or terminate the agreement.

Further, the enhanced consent requirement will detract from PIPEDA's stated goal to support and "promote electronic commerce", in that the costly and unwieldy regulatory burden created from its implementation will discourage innovative uses of personal data that to which the Proposals would be applicable.

Operational Challenges

Operationalizing the contemplated consent requirement where data is processed by third parties, whether domestically or internationally raises significant practical issues. As noted, the investment industry requires the collection, storage, processing and reporting of significant amount of data in the ordinary course of financial planning, trading on domestic and international marketplaces, portfolio analysis and optimization, clearing and settlement, and reporting to domestic and international regulators.

Given the vast amount of data involved in the investment process, and the way in which all of this 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, changes to the process will necessarily have to account for specialized processing for many of these functions, as the complexity of the investment process requires third party specialists to undertake certain required activities, and many value added functions.

Companies, particularly large ones, may have hundreds of service providers who may be using multi-jurisdictional cloud computing, making requirements for disclosure and the contemplated express consent impractical, if not impossible.

For firms, the process of initial and ongoing notification and consent, providing for opt-outs where applicable and tracking would be virtually impossible on an ongoing basis.

Currently in Canada, there are 6.6 million full-service accounts. Requiring new disclosure and consent for these existing accounts would require re-papering the 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 are potentially very detrimental for clients, as timing can often be critical in dealing in the financial markets.

In order to fulfill the enhanced consent requirement, firms would be required to monitor and seek express consent not only for their data flows, but those of their third party contractors, potentially leading to continual new disclosure and consent requests for the 6.6 million accounts they serve, many of which may have a slightly different mix of information processors serving them. This development and disclosure publication would require significant resourcing and would produce volumes of information that is counterproductive in client protection, as at a certain point, clients become overwhelmed with information and disclosure and do not read or seek to understand it.

If existing accounts are grandfathered for disclosure and consent, requiring ongoing, enhanced consent as new processors are adopted or existing processors change jurisdictions would be extremely disruptive and would introduce confusion and an overload of information and action requirements for clients. As noted, this disclosure and consent is likely to be meaningless, as clients wishing to receive services would consent as a matter of course.

Ultimately, ongoing disclosure and consent is unnecessary, as in the course of using third party processors, firms have obligations under PIPEDA and financial regulations to ensure client data is subject to appropriate data protection. The principle of accountability is much more effective in ensuring clients' data is protected than obtaining consent.

June 11 - Questions for Stakeholders (Longer term – Future law)

1. **How should a future law effectively protect privacy in the context of transborder data flows and transfers for processing?**

We believe that relying on the principle of Accountability, rather than requiring specific consent is appropriate where the transborder data flows and transfers for processing relate to standard business practices relating to the provision of the services for which the client has contracted. Given that firms are ultimately accountable for safeguarding their clients' information, the current practice of disclosing how the information will be used, and if it may be transferred across borders is appropriate and sufficient. We agree that where the use or disclosure of client information is for purposes outside the provision of the contracted services, it should be subject to a more rigorous consent requirement. This framework for client data protection is consistent with the reasonable expectations of clients.

2. **Is it sufficient to rely on contractual or other means, developed by organizations and reviewed only upon complaint to the OPC, to provide a comparable level of protection? Or should a future law require demonstrable accountability and give a public authority, such as the OPC, additional powers to approve standard contractual clauses before they are implemented and, once they are adopted, proactively review their implementation to ensure a comparable level of protection?**

It is sufficient for firms to rely on contractual or other means developed by the organizations or in accordance with industry standards to provide a sufficient level of protection. It would be wholly impractical from a resourcing perspective, at the firm level as well as at the public authority level, for firms to obtain approval for their contractual clauses prior to implementation. The number and variations of client contracts that would be subject to such approval would overwhelm any public body responsible for this function, which would impede commercial activity. In addition, the specific expertise required to understand the context and purpose of the data flows for any given industry would present insurmountable staffing challenges for such a body.

It may be helpful for the OPC to provide suggested, but non-mandatory contractual language for common situations, to assist the industry in compliance, while allowing for customization to address specific circumstances. Alternatively, the OPC could emulate the GDPR approach, providing a list of items that the contract must address, without providing specific language for those provisions.

In respect of the proactive review of implementation, this also would require significant resources with specialized training to understand the nature of data in different industries. Given that firms are ultimately accountable for issues that may arise with client data, this degree of oversight is not necessary.

3. How should a future law effectively protect privacy where contractual measures are unable to provide that protection?

The remedies under contract law, and the findings of regulators where firms have not provided the requisite reasonable data protection are sufficient to protect and compensate clients.

Conclusion

The IIAC believes that the current PIPEDA regime, underpinned by the principle of accountability and transparency is an effective means of ensuring clients' personal data is protected. Introducing additional disclosure and enhanced consent for using third party processors (domestic or international) creates significant, and likely unworkable operational barriers to the process, without corresponding client protections. In fact, an enhanced consent requirement would be detrimental to clients, as it would require them to undertake active steps increasing the cost of service and introducing risk to clients who may not be able to provide consent in a timely manner, and opening up the possibility of cyber criminals taking advantage of this barrage of requests to perpetrate crime.

We believe that clients' interests are better served by the accountability principle, which requires that firms focus their attention on the protection of client data, rather than obtaining individual consent affirmations from clients are not necessarily well informed about what they are consenting to, and ultimately are relying on the firms' diligence in protecting their data.

If there is a problem with improper use of client data, it would be more effectively addressed by requiring firms to strengthen their accountability and cyber protections.

Thank you for considering our comments. If you have any questions, please don't hesitate to contact me.

Yours sincerely,

Susan Copland