IIAC ACCVM
Investment Industry Association of Canada Association canadienne du commerce des valeurs mobilières

August 14, 2023

Director General
Financial Crimes and Security Division
Financial Sector Policy Branch
Department of Finance Canada
90 Elgin Street
Ottawa ON K1A 0G5

Via Email: fcs-scf@fin.gc.ca

Dear Sirs/Mesdames,

RE: Consultation on Strengthening Canada's Anti-Money Laundering and Anti-Terrorist Financing Regime

The Investment Industry Association of Canada (IIAC) is the national association representing investment firms that provide products and services to Canadian retail and institutional investors. Our members manufacture and distribute a variety of securities including ETFs, mutual funds, closed-end funds, and other exempt products. They provide a diverse array of portfolio management, advisory and non-advisory services. Our members service most retail investors in Canada.

The IIAC applauds the Department of Finance's efforts to improve Canada's Anti-Money Laundering and Anti-Terrorist Financing Regime (the "Regime") and is supportive of specific changes required to ensure a robust, efficient, and effective anti-money laundering and anti-terrorist financing regulatory infrastructure in order to detect and deter criminal activities and to enhance the overall credibility of Canada's commitment to combatting financial crime.

Executive Summary:

- We believe that for a beneficial ownership registry to be effective to meet transparency objectives, it should be maintained centrally by the federal government with the participation of all provincial and territorial jurisdictions.
- We do not object to the implementation of a formal "keep open" regime that is accompanied by an affirmative safe harbour defense.
- We support private-to-private information sharing with significant enhancements to PIPEDA.
- We support a government-developed and government-maintained database of PEPs and HIOs with all associated costs to be borne by the CFCA.
- We oppose the enabling of FINTRAC and other regulators to leverage their respective compliance-related findings.
- We propose adding language to define when a business relationship no longer exists.
- We proposed extending account opening identification exceptions to entities that are regulated by a non-Canadian FATF jurisdiction that have a fulsome AML regime.
- We disagree that providing a broader ability for FINTRAC to apply administrative monetary penalties to individuals of Reporting Entities, whether directors, officers or agents, would improve deterrence against non-compliance violations.
- We propose to add a monetary threshold to the STR filing criteria.

With this, the IIAC is pleased to provide the following comments in response to specific questions and issues identified in the consultation paper, on behalf of our members.

I. Federal, Provincial and Territorial Collaboration – 3.1 Beneficial Ownership

How can different orders of government better collaborate and prioritize AML/ATF issues related to beneficial ownership, [the legal profession, and civil forfeiture]?

The IIAC agrees that combating financial and profit-motivated crime is a shared responsibility between federal, provincial and territorial governments, recognizing that a key role is also held by market participants who are reporting entities, to ensure Canada does not become a haven for financial criminals; and that all parties must intensify efforts to deter, investigate and prosecute money laundering and terrorist financing activities. The IIAC further agrees that beneficial ownership transparency is vital to the success of Canada's Proceeds of Crime Money Laundering Terrorist Financing Regulations ("PCMLTFR"). A national registry that contains current and accurate information with respect to beneficial ownership will not only reduce the burden on the Regime, but it will also provide validation to IIAC members as to the accuracy and transparency of beneficial ownership information obtained by investors (as there is currently no way to validate).

However, we note that the proposal does not contemplate mandatory participation by all provinces and territories, and instead seems to be accommodative of provinces and territories who choose not to participate in a pan-Canadian registry.[1] With this, we believe that the federal and provincial governments should be heavily involved in the maintenance of information contained within the registry, and not fall on Reporting Entities to maintain the accuracy of information.

[1] Consultation on Strengthening Canada's Anti-Money Laundering and Anti-Terrorist Financing Regime, p18 [*Consultation*]

The IIAC argues that in order for a beneficial ownership registry to be effective to meet transparency objectives, the registry should be maintained centrally by the federal government with the participation of all provinces and territories[2].

II. Criminal Justice Measures to Combat Money Laundering and Terrorist Financing – 4.11 Keep Open Accounts Under Investigation

Should a legislated "keep-open" regime be implemented? How should such a regime operate vis-à-vis circumstances under which law enforcement would make a "keep open" request, the discretion of financial institutions to accept or deny the request, whether legal and reputational protections are required for financial institutions that comply with the request, and ensuring privacy rights are protected?

Personal financial account information held by financial institutions can provide valuable intelligence to law enforcement investigations when obtained in an appropriate and lawful manner, such as a production order or warrant. However, any investigation may be inadvertently disrupted, with the subject of the investigation potentially being alerted to the investigation, in the event that a financial institution closes the account, which they are currently permitted to do at their discretion, even if they are aware of an investigation by law enforcement.

It is important to understand the reasons why a financial institution may exercise their right to close an account, in particular when they become aware that an account holder is under investigation. Organizations will typically take such measures in order to mitigate the risk of financial loss and more critically, reputational damage.

In addition, regulations related to the frequency of STR reporting on accounts under investigation must be considered. A Reporting Entity should not be required to spend resources reporting on every transaction for an account under investigation and be indemnified from this reporting once a “keep open” status has been established. Significant resources are required to continuously report on activity, and it is in the Reporting Entity’s best interest to demarket and close off the relationship. If firms are compelled to maintain these relationships, we ask that STR reporting regulations be amended accordingly.

Furthermore, the request from law enforcement should be provided in written form, and should be specific, noting both that the law enforcement agency has requested that the financial institution maintain the account, as well as the purpose and duration of the request. Furthermore, there must be guidance provided on withdrawal and transfer-out request handling for the Reporting Entity should the situation arise.

Accordingly, the IIAC does not object to the Cullen Commission's recommendation[3] that a formal "keep open" regime be implemented. This would allow financial institutions to keep an account open at the request of law enforcement who wish to continue the investigation if the account is suspected to be involved in money laundering or terrorist financing activities. However, there must be

[2] Cullen Commission of Inquiry into Money Laundering in British Columbia – Final Report, Recommendation 52 [*Cullen*].

[3] Ibid. Recommendation 50.

amendments made, including an affirmative safe harbour defense[4] or other safe haven granted with the "keep open" request to shield the firm from liability exposure or reputational damage that may arise from keeping the account open.

III. Information Sharing – 6.1 Private-to-Private Information Sharing

Are there specific tools, mechanisms, or models from other jurisdictions that could be incorporated into Canadian legislation to support greater information sharing? What guardrails would best protect personal information while allowing for additional information to be exchanged between organizations?

As noted in the consultation, criminals can take advantage of a lack of information sharing between reporting entities and may attempt to engage with multiple institutions to facilitate illicit activities, where each institution only has a limited and partial view of transactions. This limits the ability of financial institutions to identify and report potential money laundering or terrorist financing activities.

While PCMLTFA has safeguards in place to ensure that privacy rights are protected in the course of FINTRAC's activities, and Canada's Personal Information Protection and Electronic Documents Act ("PIPEDA") currently permits the exchange of personal information by organizations without informed consent for the purposes of a criminal investigation or preventing fraud[5], the provisions leave it to the financial institutions to decide which circumstances are deemed appropriate, which is not sufficient to ensure the disclosure of information will be done uniformly, effectively and with respect to the individual's right to privacy under PIPEDA.

Information sharing can enhance an institution's management of its money-laundering and terrorist financing risks and can provide more effective application of AML/ATF requirements. A voluntary framework, similar to that of the USA PATRIOT Act's Section 314(b)[6], would facilitate the filing of more comprehensive STRs and build a more accurate picture of a customer's activities where potential money laundering or terrorist financing is suspected.

Therefore, the IIAC agrees that private-to-private information sharing can help reporting entities more accurately assess customer risks or identify potential suspicious activity, and is supportive of enhancements to the Regime with significant enhancements to PIPEDA[7] to strengthen and clarify the private-to-private reporting framework, including but not limited to, offering protection for firms

---

[4] *Cullen, supra* note 2. Recommendation 48.

[5] Personal Information Protection and Electronic Documents Act, PART 1 - Protection of Personal Information in the Private Sector. 7. Disclosure without knowledge or consent (3) For the purpose of clause 4.3 of Schedule 1, and despite the note that accompanies that clause, an organization may disclose personal information without the knowledge or consent of the individual only if the disclosure is (d.1) made to another organization and is reasonable for the purposes of investigating a breach of an agreement or a contravention of the laws of Canada or a province that has been, is being or is about to be committed and it is reasonable to expect that disclosure with the knowledge or consent of the individual would compromise the investigation; (d.2) made to another organization and is reasonable for the purposes of detecting or suppressing fraud or of preventing fraud that is likely to be committed and it is reasonable to expect that the disclosure with the knowledge or consent of the individual would compromise the ability to prevent, detect or suppress the fraud.

[6] USA PATRIOT Act Section 314(b) permits financial institutions, upon providing notice to the United States Department of the Treasury, to share information with one another in order to identify and report to the federal government activities that may involve money laundering or terrorist activity. Financial institutions wanting to do so may notify the United States Department of the Treasury by submitting a notification form with the required information through FinCEN's (Financial Crimes Enforcement Network) secure electronic information sharing system.

[7] *Cullen*, supra note 2. Recommendation 48.

from liability or sanctions from inadvertent or potential PIPEDA violations, when information is shared in good faith for purposes of assisting with the identification of suspected money laundering and terrorist financing activities.

IV. Information Sharing – 6.2 Public-to-Private Information Sharing – Database of Politically Exposed Persons and Heads of International Organizations.

Should the government create and maintain a database of politically exposed persons (PEPs), heads of international organizations (HIOs), and their family members and close associates? Should the government charge an access fee to help offset costs of such a registry? Does this proposal raise any privacy considerations? Is there a need for such a database given the existing resources and other databases available?

Currently, all financial services firms and institutions have an obligation to treat PEPs as high risk and therefore they extend significant resources on monitoring. Without a national database of PEPs and HIOs (and their family members and close associates), organizations must utilize third-party services to facilitate their reviews and investigations. Firms may use certain free services like Namescan and the lists of the Office of Foreign Assets Control (OFAC) however neither maintains a fulsome or comprehensive PEP list. Instead, they publish multiple lists including Sanctions and Specially Designated Nationals which firms use to assist with monitoring required under PCMLTFR. Firms may also use paid PEP screening services such as Thomson Reuters, Dow Jones Risk and Compliance, LexisNexis Risk Solutions and others. While fulsome, there is an absence of consistency and comparability of all the paid PEP screening services, and the costs are often prohibitive.

Accordingly, the IIAC is in favour of a government-developed and government-maintained database of PEPs and HIOs against which firms can scrub their client base or portfolios. Development should include fulsome data governance standards in order to manage any privacy-related risks. Further, with the government's commitment to create a new, dedicated lead enforcement agency, (the Canada Financial Crimes Agency (CFCA)), we believe the CFCA should be responsible for the maintenance of the PEP and HIO database, and the costs of development and ongoing maintenance should be borne by that entity.

V. Information Sharing – 6.3 Public-to-Public Information Sharing – Sharing Information Between FINTRAC and other Regulators

Should the government amend the PCMLTFA to provide FINTRAC the ability to leverage findings from other regulators in its compliance examinations and share FINTRAC compliance information with other regulators to inform compliance assessments and help improve supervisory strategy? What impact would this have, if any, on reporting entities' relationships with their other regulators, including in terms of openness to share information?

As part of FINTRAC's risk-based compliance program, FINTRAC conducts examinations of its reporting entities to ensure that businesses are fulfilling their compliance obligations. In certain circumstances, as a means of efficiency, exams have been conducted concurrently with other regulatory bodies. However, FINTRAC cannot use compliance-related findings assessed by other regulators to inform its own compliance assessments and must make non-compliance findings on its own. FINTRAC is fully

empowered to address AML/ATF concerns through its policies, audits, enforcement powers, etc. There are no additional protections provided by other regulators that cannot be provided through FINTRAC. Rather, the involvement of other regulators provides unnecessary duplication and administration.

Accordingly, the IIAC is opposed to enabling FINTRAC and other regulators to exchange their respective compliance-related findings for purposes of leveraging those findings to inform compliance assessments and supervisory strategies. The IIAC is concerned that this proposal is beyond the scope of the current consultation and would not have any demonstrable benefit to strengthening Canada's anti-money laundering and anti-terrorist financing regime.

VI. Scope and Obligations of AML/ATF Framework – 7.4 Streamlining Regulatory Requirements – End Period for Business Relationships

Should the concept of "business relationship" in the PCMLTFA and its Regulations be clarified to specify when it is considered to have ended? How could the end period for "business relationship" be made consistent and applicable across all reporting entities? Should a proposed end period correspond to existing obligations to keep records (e.g., 5 years from account closure or last transaction)?

Once a client has closed their last account with a reporting entity, the risk associated with that relationship is relatively low. The definition within FINTRAC regulations currently considers the business relationship to continue for a period of 5-years post-last account closure. Given that there is no ability for a transaction to occur in a closed account, and there would be no KYC information updates - the potential for material information leading to a suspicious activity and reasonable grounds to suspect money laundering is minimal, if not eliminated entirely.

The PCMLTFR currently includes a definition describing the circumstances in which a business relationship is considered to be entered into. However, there is no defined set of circumstances to when a business relationship has ceased. Accordingly, below is suggested language:

“A Business Relationship ends once the last account is closed with a Reporting Entity whereby transactions can no longer occur."

The benefit of this change in criteria is that once reporting entities are relieved of a Business Relationship they are also relieved of the obligation for ongoing monitoring. Without transactions or KYC updates taking place in the account, the task of reviewing these closed accounts on an ongoing basis becomes merely an administrative task. Adding this language would allow reporting entities to focus their resources on the area of highest risk, and not burden themselves with this low value, low risk obligation.

The IIAC proposes adding the above noted language to which reporting entities can be uniformly certain that a Business Relationship no longer exists - and ongoing monitoring no longer needs to take place.

VII. Scope and Obligations of AML/ATF Framework – 7.4 Streamlining Regulatory Requirements – Opportunities to Streamline Other AML/ATF Obligations

What are other opportunities to streamline AML/ATF requirements?

As the financial sector and AML/ATF risks evolve and change over time, we agree that it is worth reviewing whether AML/ATF obligations for reporting entity sectors could be streamlined to reduce regulatory burden in appropriate areas. One such area could be the identification of exceptions on account opening. Specifically, we believe there it would be justifiable and appropriate to consider that in requiring the identification of entities, and individuals authorized for those entities, there should be exceptions granted when entities are regulated by securities regulatory authorities outside of Canada, when there is a comparable AML regime, and/or for those that are within FATF jurisdictions in good standing. This would allow Reporting Entities to have the flexibility to apply a risk-based approach to their account opening processes.

The IIAC proposes extending an exception to the general identification requirements for foreign regulated entities when the foreign jurisdiction has a robust AML regime and/or when they are within a FATF jurisdiction in good standing.

VIII. Regulatory Compliance Framework – 8.1 Modernizing Compliance Tools – Issuing Administrative Penalties Against Individuals

Should the government amend the PCMLTFA to grant FINTRAC the authority to levy administrative penalties against directors, officers, and agents within an entity in certain cases of violations of the PCMLTFA? Under what circumstances should FINTRAC be authorized to levy a penalty against directors, officers, or agents?

Under the PCMLTFA, if a criminal offence for non-compliance is committed (either by a person or an entity) any director, officer, or agent associated with that entity or person is held liable for the committed offence. FINTRAC does not otherwise have legislative authority to issue administrative monetary penalties against directors, officers, and/or agents within an entity (except in the case of a sole proprietorship), and we believe this is appropriate. When there is a failure within a Reporting Entity, it is the collective responsibility of the entire Reporting Entity to prevent money laundering/terrorist financing and therefore imposing administrative penalties on individuals would inappropriately put the focus of fault on individuals rather than the issues within the Reporting Entity that led to the compliance failures.

The IIAC disagrees that providing a broader ability for FINTRAC to apply administrative monetary penalties to individuals of Reporting Entities, whether directors, officers or agents, would improve deterrence against non-compliance violations, and hence we are opposed to amending PCMLTFA to grant FINTRAC this authority.

IX. Regulatory Compliance Framework – 8.2 Effective Oversight and Reporting Framework – Reporting Framework

How can the government assist reporting entities in fulfilling their reporting obligations in a manner that provides FINTRAC with information necessary to prepare financial intelligence? How can the government clarify reporting obligations?

The current regulations place the onus on reporting entities to file a Suspicious Transaction Report (STR) whenever there are reasonable grounds to suspect money laundering has occurred, regardless of dollar

value. In reviewing the statistics published in the Cullen Commission Report[8], it could be concluded that FINTRAC is either receiving a large number of filings not worthwhile to pursue, or potentially they are unable to keep up with the influx of STRs submitted to them.

Reporting entities and FINTRAC alike have a desire and an obligation to Canadians to do their part to combat money laundering. It is with this in mind that we propose to add a monetary threshold to the STR filing criteria in addition to the reasonable grounds to suspect money laundering in order to help focus the reporting to be on larger-scale money laundering transactions. Doing so would help facilitate a coordinated risk-based approach across FINTRAC and reporting entities and allow FINTRAC to concentrate its resources on higher value suspicious transactions.

By way of additional general comments, the IIAC appreciates the efforts to ensure that developments and enhancements to the Regime be made in accordance with new and emerging risks, domestic market developments, and elevation of international standards. The IIAC also commends the acknowledgement that, "despite continued improvements to the legislative and regulatory AML/ATF framework, achieving operational effectiveness remains a persistent challenge for you"[9], and trusts that currently and under the new Regime, you will extend this recognition to reporting entities. Last, we hope that any increase in obligations on reporting entities will occur with due consideration to implementation timelines and current regulatory burdens.

The IIAC is grateful for the opportunity to comment. We would be pleased to address any questions or concerns in respect of our comments; they may be directed to the undersigned.

Sincerely,

Investment Industry Association of Canada

[8] *Cullen*, *supra* note 2. Chapter 7 The Canadian Anti-Money Laundering Regime, p205. In 2019–20, reporting entities in Canada submitted a total of 31,417,429 individual reports to FINTRAC; Compared to the United States (US) and United Kingdom (UK), there was 12.5 times more reports in Canada as compared with the US and 96 times more reports as compared with the UK; Despite the huge volume of information collected under the federal regime, FINTRAC made only 2,057 "unique" disclosures to law enforcement bodies in 2019–20 and only 1,582 of these disclosures were directly related to money laundering (with 296 related to "terrorism financing and threats to the security of Canada" and 179 related to "money laundering, terrorism financing and threats to the security of Canada"); FINTRAC received 2,519 voluntary information records from law enforcement agencies across the country in the 2019–20 fiscal year; it seems likely that most of the 2,057 "unique" disclosures made to law enforcement in 2019–20 were made in response to these requests.

[9] *Consultation*, *supra* note 1, p6.