Canadian Web3 Council

August 1, 2023

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

To Whom it May Concern,

The Canadian Web3 Council (CW3) is pleased to respond to the Government of Canada's Consultation on Strengthening Canada's Anti-Money Laundering and Anti-Terrorist Financing Regime (Consultation Report). We consent to the public disclosure of our comments.

The CW3 is a non-profit trade association founded by industry leaders to work constructively with policymakers and establish Canada as a leader in web3 technology[1]. The CW3 represents organisations that have made a critical impact on the development of web3 technologies across the globe, and who are committed to responsibly building and innovating in Canada. Our membership is diverse, ranging from hackathon organizers to financial products, trading platforms and investors, and open-source blockchain projects.

Executive Summary

CW3 and its members understand the importance of the Government of Canada's efforts to strengthen Canada's Anti-Money Laundering (AML) and Anti-Terrorist Financing (ATF) regime. As web3 technology becomes more mainstream and there is greater adoption by Canadians, AML, ATF as well as fraud prevention and financial crime disincentives are critical to the legitimacy and growth of this industry.

We encourage Canada to use its global leadership role to be strategic and evidence based when effecting change to rulemaking. **We welcome the opportunity to engage with the government and agencies to develop specific proposals that can both strengthen the current AML/ATF framework and which are tailored to fit the crypto sector.**

[1] At its core, web3 technology aims to enable direct interactions between users without relying on intermediaries. It emphasizes the use of decentralised applications (dApps) that run on blockchain networks, where data and processes are distributed across a network of nodes, making them resistant to censorship, manipulation, and single points of failure. Overall, web3 technology represents a paradigm shift towards a more decentralised, open, and user-centric internet, empowering individuals and communities with greater control over their digital lives.

Many of CW3's members cover a wide range of activities within the FinTech[2] space. Many are registrants or reporting entities under the Proceeds of Crime, Money Laundering and Terrorist Financing Act and associated regulations (PCMLTFA/R), as well as regulated under other Canadian or provincial/territorial laws or regulations. They may be money service businesses (MSB), securities dealers, payment service providers and/or a crypto trading platform[3]. MSBs and securities dealers are required to have written policies and procedures to detect, prevent and report illicit criminal activities such as money laundering and terrorist financing, as well as adhere to sanctions laws.

We support the work that the Government of Canada is undertaking in its AML/ATF initiatives. We set out below our thoughts on certain aspects of the Consultation Report, in particular as it relates to virtual currencies and other digital assets as well as virtual currency service providers, Detailed responses, by chapter, are set out further in this letter.

1. We encourage Canadian regulatory and law enforcement agencies to work with the web3 industry in Canada to better understand web3 technologies, its use cases and potential solutions to help inform a suitable regulatory framework for virtual assets and Virtual Asset Service providers (VASPs). We recommend creating flexibility in any amendments to the PCMLTFA/R to allow for industry developments and innovation.

2. We believe there are significant issues of de-risking of VASPs in Canada. We highlight the negative impact to innovation, competition and financial inclusion as a result of de-risking activities whereby VASPs may be denied financial services simply because they are deemed to be in a high risk sector. We believe there are well-run and well-governed VASPs who have implemented strong AML/CTF measures[4]. The current risk-based framework should be able to distinguish well-run companies. We question why Financial Institutions (FIs) are permitted to apply a "one-size fits all" approach to their risk assessments which results in denial of financial services to specific industry sectors. We welcome an empirical study of the impact of de-risking activities by certain reporting entities and registrants which should then be used to inform guidance on effective risk assessment and risk management framework. See paragraph 39 below.

3. We support evidence-based policymaking. In certain evolving sectors, such as decentralised finance (DeFi) and non-fungible tokens (NFTs), it is critical to consider the evidence[5] and consult with industry, and globally, before deciding on an AML/ATF regulatory framework for

---

[2] Developments in technology such as blockchain, artificial intelligence, digital assets, distributed ledger systems, the metaverse, and decentralised finance, including decentralised autonomous organisations (DAOs) (collectively, for the purpose of this response, "FinTech")

[3] The Canadian Securities Administrators (CSA) use the term crypto trading platform to categorize certain trading activities in crypto. Globally, a CTP would be considered a virtual asset service provider (VASP).

[4] To satisfy their obligations under the PCMLTFA/R, members have implemented an AML/ATF compliance program that includes requirements for customer identification, record-keeping and transaction reporting.

[5] The evidence to be collected would include the sector (collectibles, real estate, music etc), monitoring for the relative size of transactions, market activities and the potential for a NFT trading platform to be used to conduct illicit activities. For example, Elliptic used "data-driven analysis into the prevalence of money laundering, terrorist financing, scams and sanctioned entities. It found that these financial crimes represent a small but notable portion of overall NFT-related trading activity." NFT and Financial Crime Report 2020 Link here. We recommend continuous monitoring of this sector and for regulators to consider the use of technology solutions to address such risks.

these sectors given the range of use cases and sectors[6]. This would ensure that AML/ATF recordkeeping and reporting obligations are proportionate to the risks and, more importantly, that the measures will help support the effective enforcement of the AML/ATF regime in Canada.

4. We believe the unique characteristics of blockchain technology (i.e. transparency) together with enhanced data analytics tools and insights provide an opportunity for industry, regulators and law enforcement to enhance their approach to supervision and investigation. Moreover, improvements to the quality of reporting together with increased digital competency using analytical tools can help secure better enforcement outcomes. We encourage regulatory and law enforcement agencies to work with industry members to conduct training programs[7] and implement analytic tools to achieve better regulatory outcomes that lead to the detection, prevention, reporting, and prosecution of ML/TF offences.

5. We favour minimising complexity to reduce regulatory burden. Regulatory burden creates barriers to entry, impedes innovation and reduces productivity (especially for small and medium enterprises (SMEs))[8]. We offer the following recommendations to reduce regulatory burden and increase productivity as it relates to AML/ATF:

    a. We encourage the government to work with its global partners in establishing a global database for politically exposed persons (PEP)/head of international organisation (HIO) databases. We believe that tackling this initiative through a global effort can be more effective than having the Government of Canada undertake this. We recommend policy makers and regulators consider partnering with industry to find a Public/Private solution to create a global PEP/HIO database. (See paragraph 15 below.)

    b. Streamline the inter-agency coordination and collection of information for law enforcement purposes through a single point of collection and mutual cooperation agreements. This would serve to remove duplicative reporting by reporting entities and duplicative efforts by the respective agencies.

    c. We encourage all regulators to adopt a global taxonomy for digital assets and digital asset service providers. The use of the terms “virtual assets” and “virtual asset service providers” (VASPs) are used by the FATF and would encourage it to be adopted in the PCMLTFA/R. Using common language is a necessary first step towards global regulatory harmonisation and in defining an appropriate regulatory perimeter for emerging virtual assets and VASPs.

---

[6] In February 2023, the FATF released a report on Money Laundering and Terrorist Financing in the Art and Antiquities Market, which includes a section on digital art and non-fungible tokens (NFTs). Link Here

[7] Canadian Web3 Council, Onboard to Web3 Link here.

[8] We submit that the regulatory burden on digital asset service providers will have a negative impact on productivity similar to the paperwork burden. See *The Impact of Regulatory Compliance Costs on Business Performance*, a study by Innovation, Science and Economic Development Canada on Paperwork Burden Reduction. “Empirical findings reveal that the regulatory burden faced by an SME is affected by its size and revenue. The larger a firm's size and revenue, the lower the intensity of regulatory compliance costs on that firm. There is a negative relationship between a firm's regulatory burden and its productivity. A one percent rise in the intensity of regulatory compliance costs is associated with a 0.1 percent decline in a firm's labour productivity.” Link Here

d. We favour an emphasis on higher quality of reporting (rather than quantity). We encourage the Government of Canada to work with industry members to find solutions that will improve the effectiveness of AML/ATF programs, quality of reporting and productivity[9].

6. We are not aware of any significant issues with the current reporting entity vs. registration framework under the PCMLTFA/R and do not believe it is necessary for universal registration of all reporting entities with FINTRAC. A reporting entity has similar obligations and are subject to FINTRAC compliance and enforcement as those that are registered. As noted below (in paragraph 37) registration makes sense in those situations where an entity is not otherwise registered.

7. We support the Government of Canada's efforts to improve communications and methods of communicating with the private sector and between different public sector agencies. The use of secure methods of communicating help to maintain privacy of personal information and facilitate speedy dissemination across all players. Data collection must be purposeful and focused to avoid imposing regulatory burden on registrants/reporting entities. We are encouraged by the Canadian Government's efforts to keep privacy considerations as a key priority and encourage the constant reassessment of information gathered to ensure we are only collecting and storing what needs to be collected for investigation and enforcement requirements.

8. We support the use of a regulatory sandbox to test new technologies or systems that might support open-banking and other payment systems. Supporting innovation may encourage development of regtech and fintech solutions that enhance transaction and identity monitoring for AML/ATF activities, in addition to usage for law enforcement.

We are pleased that Canada plays such a major role in the Financial Action Task Force (FATF). **We ask the Canadian Government to recognize that the VASPs and the web3 industry can be an alternative to traditional financial markets currently dominated by large incumbents. We ask that the Canadian Government also use its leadership position to influence policy on the international stage[10].**

[9] The "Final Report of the Commission of Inquiry into Money Laundering in British Columbia" June 2022 (the "Cullen Commission) (link here) indicated that the current intelligence gathering regime under the PCMLTFA/R results in high-volume, low-value reporting.

[10] CW3 can provide the government and agencies with a better understanding of the technology and its use cases and its intersections with global payment systems. This knowledge can help Canada be strategic in taking a leadership role on international committees (BIS, IOSCO etc.) to create a global AML/CTF framework in a manner suitable for a modern global financial, capital and crypto markets.

General

CW3 members understand the importance of AML/ATF activities and meeting its requirements under the FATF standards[11]. We encourage the Government of Canada to take a holistic approach to AML/ATF activities for virtual assets and VASPs and to engage with industry at all stages of rule-making.

We also ask that the Government of Canada consult with industry to support SMEs when drafting amendments to the PCMLTFA/R. We emphasise the importance for SMEs to be represented on such matters, given that research indicates that the regulatory costs of compliance has a greater impact on SMEs than on larger FIs[12]. A significant number of reporting entities and registrants under the PCMLTFA/R are considered SMEs. SMEs typically have limited resources and may take longer to complete investigations and reporting than larger entities. Continuous improvements for cost-effective technology solutions by the government and industry should be encouraged.

A strong AML/ATF regime is important to support an innovative, technology driven Fintech industry in Canada. We support the work done by the Standing Committee on Industry and Technology in its report "Blockchain Technology: Cryptocurrencies and Beyond"[13]. We encourage revisions to the PCMLTFA/R to be done in such a way as to not impede innovation and that could be used by traditional FIs and service providers as an excuse to stop them from interacting with players in the Fintech space. In particular, the following recommendations from the report are considered vital when legislators amend the PCMLTFA/R, Criminal Code, and any other laws or regulations that impact the use and adoption of blockchain technologies and encourage broad industry consultation on these matters.

- Recommendation 2 – that an individuals' right to self custody should be protected and that ease of access to safe and reliable on and off ramps should be defended and promoted.
- Recommendation 5 – that the Government of Canada pursue opportunities for international cooperation in the development of blockchain regulations and policies.
- Recommendation 10 – that the Government of Canada adopt measures for access to banking and insurance services for blockchain firms.

We applaud the Canadian Government in its past consultative activities and industry outreach and encourage the expansion of the Advisory Committee on Money Laundering and Terrorist Financing to include other industry associations, such as the Canadian Web3 Council, among others, for virtual

---

[11] The Financial Action Task Force's (FATF) 2021 follow-up report (link here) shows that Canada has made significant progress in meeting its requirements under the FATF standards. As it relates to virtual assets and VASPs, and wire transfers, Canada has been re-rated as "largely compliant".

[12] "Empirical findings reveal that the regulatory burden faced by an SME is affected by its size and revenue. The larger a firm's size and revenue, the lower the intensity of regulatory compliance costs on that firm. There is a negative relationship between a firm's regulatory burden and its productivity". See *The Impact of Regulatory Compliance Costs on Business Performance*, a study by Innovation, Science and Economic Development Canada on Paperwork Burden Reduction. Link Here

[13] Blockchain Technology: Cryptocurrencies and beyond" Report of the Standing Committee on Industry and Technology, June 2023 Link here.

currencies and virtual currency service providers. We encourage continuous outreach to industry, including joint outreach with other agencies and support more public awareness campaigns to Canadians in general on types of ML/TF typologies and how and where to report them.

Chapter 3 - Federal, Provincial and Territorial Collaboration

1. We support the federal, provincial, territorial and municipal governments, and various departments/agencies of each, working together to reduce regulatory burden and the duplication of activities, consolidate screening information, streamline collection and submission of information and generally enhance the effectiveness and efficiency of the AML/ATF regime in Canada.

   We support the Government of Canada's efforts to develop a Canada wide beneficial ownership database and encourage provincial and territorial governments regarding entities incorporated in their jurisdiction. The lack of a database creates significant delays in onboarding corporate clients, enhanced due diligence and investigations. Once established, we would be supportive of it being expanded to trust and partnerships.

Chapter 4 - Operational Effectiveness

2. Public awareness in general is critical to raise the profile of AML/ATF issues. Many Canadians are not aware of the scope of activities that encompass AML/ATF activities, including third-party money laundering and CW3 fully supports public awareness campaigns to help the general public to recognize and how and when to report activities to the appropriate law enforcement agency, FINTRAC or the new Financial Crimes Agency. A whistleblower program is one mechanism that can be useful[14].

3. We note that some economically motivated schemes are perpetrated by actors outside of Canada. Strengthening international cooperation and information sharing between law enforcement, Financial Intelligence Units (FIUs), Tax authorities, and others who have a vested interest, is encouraged to detect, deter, prevent, and prosecute economically motivated schemes perpetrated by actors outside of Canada. To the extent that the target of changes to the PCMLTFA/R are companies or other actors who are not operating in compliance with Canadian laws, the proposed reforms could be beneficial for the security of Canada's financial system.

4. Web3 companies are willing to comply with lawful authorizations to turn over subscriber data. This should be a warranted process involving judicial authorization, in the same way as an internet service provider would turn over subscriber data. Any move to limit the judicial rigour, or to have some sort of "workaround warrant" or policy for exigent circumstances will cause a decrease in consumer confidence and will have the effect of driving some consumers to offshore platforms that are not regulated.

[14] See Ontario Securities Commission whistleblower program. Link here.

5. There are conflicting views on the seizing or restraining of digital assets for evidentiary purposes. On one hand, there may be no benefit to seizing or restraining digital assets for evidentiary purposes if the digital assets are held through a public digital ledger that blockchain systems use, as the evidence is available to everyone. Public blockchains are uniquely amenable to investigation, unlike private IT systems or private blockchains as the information is transparent and available publicly to anyone, without a warrant or even permission. On the other hand, virtual assets also have a stored value assigned to the data[15]. Off-chain data such as self-custodied/un-hosted wallets or a custodied account structure, with sub-addresses, would require different mechanisms as access to private keys is necessary. While there may be an extra element of value associated with blockchain data, blockchain data should not be considered differently than any other data under legislation. Legislation proposed in this area should be technologically neutral as innovation in this space will move faster than Parliament's ability to legislate.

6. Web3 members regularly respond to production orders and have not seen any technical obstacles to their use vis-a-vis customer accounts, wallet addresses or sub-addresses. We welcome changes that streamline this process and eliminate issues that currently impede law enforcement's ability to pursue criminals. We support the need to explicitly set out the requirements for the issuance of production orders where entities operate within and outside of Canada, notwithstanding the inherent limitations of such orders. We do not see any drawback to changes to the Criminal Code that fix technical problems that may exist, and encourage industry consultation to assess use cases.

7. The Crown's obligation to establish a pattern of criminal activity or income that exceeds lawful sources in the rebuttable presumption provision is considered sufficient. Given the cross-entity, cross-border nature of digital assets, it can be challenging to draw a conclusion based on information from reporting or regulated entities on an individual basis. We believe the transparency of the blockchain together with analytical tools can be of assistance to law enforcement and prosecutors.

8. We support the use of "keep-open" accounts as well as "Stop Withdraw Orders" (SWO) to stop a customer from using their account while investigations are in progress. The SWOs could be used to prevent a customer from being able to use the account to transfer money or virtual currency to any other place, but still allow them to continue using the account in other ways. This measure would be less harmful to law-abiding customers, while ensuring that funds are available for recovery if the person is later determined to have committed a crime. SWOs are an appropriate balance between the needs of the law enforcement and the presumption of innocence until proven otherwise. For regulated platforms in Canada, SWOs facilitate ease of implementation and management and they could assist law enforcement if designed such that the target only finds about the order when they go to withdraw, which would prevent them from being alerted to the investigation.

[15] See Forensic Science International: Digital Investigation, "A comprehensive forensic preservation methodology for crypto wallets", October-December 2022. Link here.

Clarity around the“keep-open” or SWOs regime would be critical. We encourage the development of evidence based standards, with appropriate and well-defined safeguards, to ensure consistency in execution and operation of SWOs or “keep-open” requests. Guidelines should be developed setting out in detail when “keep-open” or SWOs are to be used, monitored (by the registrant or reporting issuer, as well as law enforcement), and the mechanisms for implementation, as practices may differ between entities and between reporting entity groups. Privacy rights must be clearly addressed so that the registrant or reporting entity is not required to exercise judgement when complying with “keep open” or SWOs.

9. Where seizure and restraint of digital assets is necessary, we support the holding of these seized or restrained digital assets in a custody/in trust for/notationed account at a regulated crypto platform or custodian.

10. We fully support the adoption of legal and reputational protections for financial institutions as well as securities dealers, money service businesses and other applicable registered or reporting entities when they are complying with investigative demands or court orders.

Chapter 5 - Canadian Financial Crime Agency (CFCA)

11. CW3 supports an expanded scope of the CFCA to the extent that the CFCA could harmonise and centralise the collection and use of information and to collaborate inter-agency for law enforcement purposes. The current system requires reporting to multiple government agencies and law enforcement, often results in the filing of duplicate information and adds to regulatory burden. Canada needs one central reporting repository for AML and ATF reporting and economic sanctions and as FINTRAC is currently doing much of this already, expanding to include the other reporting would likely be the most effective.

    We understand the current proposal is to bring together, under one roof, existing law enforcement resources of the RCMP, the intelligence capabilities of FINTRAC, and expertise of the Canada Revenue Agency. We encourage the Government of Canada to look more broadly at coordinating activities with provincial and municipal law enforcement agencies as well as provincial and territorial securities regulatory authorities and consumer protection agencies. We encourage Canada to look at the recent changes to Europe’s AML regime, focusing on a centralised AML authority, consistent application of rules and verified information about beneficial owners.[16]

    All efforts to educate the public on financial crime threats are encouraged. Coordinating and partnering with industry across a variety of sectors could provide additional perspectives on financial crimes.

[16] European Parliament New EU Measures Against Money Laundering and Terrorist Financing. March 2023. Link here.

Chapter 6 - Information Sharing

12. A comprehensive assessment of private to private information sharing should be undertaken. Globally, private to private information sharing is rapidly being adopted, including ID verification, given the move to enhance the global payment systems, Canada's AML/ATF regime should take note of these jurisdictions and the information sharing protocols in place.

13. We support the continued adoption and development of technology solutions by both FINTRAC and law enforcement for communicating with all registered and reporting entities, such as the use of secure portals, with notifications, rather than relying on email communications. There should also be a mechanism for the government to share information fairly to all affected reporting or registered entities[17]. However, as information sharing increases, privacy remains a key consideration. We support mechanisms that require anonymized and standard data transmission. To improve productivity, information should be made available in digital formats, with sufficient detail, so that it can be ingested into automated systems and analytical models in order to quickly act to disrupt bad actors.

14. We are encouraged by the Canadian Government's efforts to keep privacy considerations as a key priority and encourage the constant reassessment of information gathered to ensure law enforcement is only collecting and storing what needs to be collected for investigation and enforcement requirements. Personal information must be transmitted and stored in a secure manner and we encourage all agencies to adopt the principle of least privilege for its IT security infrastructure.

15. We support the creation of a central database of PEP and HIOs to enhance regulatory compliance. The database must allow for fair access by all industry participants and law enforcement. We do not believe that fees should be charged for this access as it does not promote fairness to SMEs. We also encourage more guidance around risk assessments and enhanced due diligence and ongoing monitoring with respect to higher risk PEPs and HIOs as there can be unintended consequences such as a financial institution withdrawing or denying banking services to sitting members of parliament (e.g. the U.K.). See comments below on de-risking. Domestic PEPs may not be as high risk as PEPs from other jurisdictions. We recommend that there be notice periods if lenders want to close an account and more information about why the action has been taken. There should be a dispute resolution mechanism at the reporting entity/registrant level.

16. It is common practice for industry to use publicly available information to complete risk assessments and investigations. We agree that FINTRAC should have the ability to use this information for their analysis and assessments; however the source of the information must be

[17] For example, when the Emergencies Act was invoked in February 2022, the RCMP issued an order that prevented regulated financial services such as crypto asset exchanges from facilitating any cash-out, transfer or storage operations with specified listed wallets. While the obligation under the order applied to all regulated MSBs that dealt with crypto assets, the information was not distributed directly or equally to all affected parties, resulting in confusion and delays in enforcing the order. Further, some crypto exchanges reported that some FIs wanted the information as they too had the ability to track Crypto related to some of their MSB clients. It should be made available to all regulated entities that deal in crypto.

assessed and independently verified during the investigation process. We support amendments that reduce the regulatory burden and foster transparency, including the acquisition of administrative datasets from federal and provincial governments. There should be guidelines to minimise the collection and transmission of information to only that necessary for law enforcement purposes.

17. We would encourage the Canadian government to work closely with other federal, provincial and territorial regulatory agencies to coordinate compliance reviews, reporting obligations and filings in order to reduce regulatory burden and create efficient review processes of reporting entities. For example, the securities regulatory authorities perform registration and compliance reviews of exempt market dealers. As AML/ATF is part of the risk to a business, the securities regulators perform reviews upon registration and periodically through compliance reviews. Sharing of information and aligning reviews as they apply to AML/ATF improves efficiency of the review processes and reduces regulatory burden on registrants and reporting entities.

Chapter 7 - Scope and Obligations of AML/ATF Framework

18. Payment Service Providers. Many money service businesses (MSB) could also be considered PSPs and there should be a coordinated approach in terms of obligations and reporting. A comprehensive review of current legislation and a risk assessment of PSPs should be undertaken prior to any changes to the PCMLTFA/R. This reduces the possibility of being registered in more than one category and therefore possibly having differing requirements which could increase costs and create confusion and delays in reporting. We encourage the use of a single taxonomy for virtual assets across different legislation and regulatory frameworks.

19. Virtual Currency, Digital Assets, and Technology-Enabled Finance. We note that the FATF issued a report "Targeted Update on Implementation of FATF standards on Virtual Assets and Virtual Asset Service Providers" in June 2023[18]. We encourage the government to consult with industry in the development of these laws and regulations, prior to their enactment. The PCMLTFA has been expanded significantly in recent years and should be broad enough to address the risks of innovation and new technology. Consistency with global standards can decrease regulatory burden however, we believe Canada should seek harmonisation to the extent that the resulting laws are sensible and practical. For example, unique challenges exist in the implementation of the travel rule, which are not limited to VASPs and we encourage the Government of Canada to work with service providers including VASPs to address these challenges.

20. New FinTech products or services. We note that FATF have identified DeFi, unhosted wallets and peer to peer transactions and NFTs as market developments and emerging risks. A proportionate and technology-neutral approach to rule making is generally accepted to be the best legislative model with respect to new technologies as laws that address specific technologies are likely to create gaps that a technology-neutral approach does not. Further, it is unclear whether legislative changes are even necessary to support AML/ATF activities in relation to the metaverse or

[18] FATF, Targeted Update on Virtual Assets and VASPs, June 2023. Link here.

FinTechs in general, as the existing framework may adequately address these products or services.

We support an evidenced-based approach to assessing risks of new FinTech products or services, prior to adopting any changes to the PCMLTFA/R. Technological developments such as Anonymity Enhancing Coins/Privacy Coins, crypto-mixers and DeFi are global in nature and occur online in ways that are difficult to block or even monitor. Prior to including these technologies and services under the PCMLTFA/R we encourage the government to assess those factors that indicate the relative risk of specific platforms and services providers and work to ensure regulations are evidence based, proportionate to such risks and involve clear definitions of the processes and providers they are meant to cover. We suggest working with Canadian registrants/reporting entities for support on specific AML/ATF issues related to new Fintech products or services.

21. Metaverse. While artificial intelligence and the metaverse may add unique elements of risk that may also need to be addressed, the metaverse is a neutral technology platform, much the same way as, for example, Amazon Web Services (AWS). Virtual worlds may be a different format but they do not change the nature of the activities that might take place within them. If MSBs are operating within metaverses then they are still operating as MSBs. Cross-border issues would be similar to those that exist currently. Artificial intelligence is very broad and touches many areas of law. AML/ATF rulemaking should not be considered in isolation of the intersections with other legal and regulatory frameworks such as privacy, data governance, cybersecurity and human rights.

22. Virtual currency and digital assets are borderless and the seamless transfers of value across jurisdictions is a key benefit to their use. As the world moves to adopt open banking and real time payment rails, cross border transfers will increase. A number of countries do not prohibit the use of crypto-mixers/crypto-tumblers. If and when such time as mixers and tumblers are prohibited globally, restricting the receipt of funds in Canada may target legitimate transactions as not all users of virtual assets are aware of when mixers and tumblers are being used. However, if there is evidence of abuse, there may be value in restricting the transfer to mixers and tumblers.

23. The vast majority of current AML/ATF obligations under the PCMLTFA/R are technology neutral. However, we note that the travel rule is one obligation that requires technology solutions that are not yet fully compliant or where there are interoperability issues when it comes to Virtual Currencies and domestic EFTs transactions. Central elements of the travel rule's requirements are for originator and beneficiary information to remain with the transaction from inception point to end point. The global payment systems are becoming more open, with less intermediation, and the volume and speed of transactions are increasing. Being able to rely on identity verification for transfers/transactions between registered/reporting entities will be a key element in the development of open banking. In the current environment, requiring "know your client" (KYC) verification at every point in the payment process creates friction and is an impediment to real time settlement. However, it is also important to respect the laws around the secure transfer/sharing of personal data across jurisdictions.

24. We encourage the government to regularly consult with the industry, beyond the existing Department of Finance Advisory Committee on Money Laundering and Terrorist Financing[19], to address technology and implementation issues, especially as it relates to virtual assets and VASPs. Technology solutions must take into consideration risk assessments, varying sizes of entities within this industry and cost constraints. Canada needs to balance innovation in this space, allowing small players access to grow without being absorbed into large financial institutions, with AML/ATF regulation. As noted below, smaller companies may be doing things manually versus larger regulated entities. This impacts the time it takes to investigate, file reports, and take action when required by law enforcement.

25. High Value Goods. We believe that a robust and secure NFT industry must be predicated on the principles of consumer protection and safety and that comply with laws and regulations that support innovation while ensuring that NFT trading is not abused or used for illicit purposes. While NFTs are not included under the PCMLTFA/R, members of CW3 have voluntarily adopted certain AML/ATF measures (e.g. customer due diligence, sanctions screening etc) as part of their business practices and is a critical tool for consumer protection and building and maintaining trust. As the scope and application of the PCMLTFA/R is contemplated, we recommend a detailed review of industry practices, such as how funds to acquire or sell NFTs, crypto or fiat, are received and stored as many NFT platforms utilise regulated financial institutions or digital asset platforms. Any expansion to the scope of the PCMLTFA/R should be based on evidence that supports an expanded risk framework, be proportionate to the risk, and must consider the emerging status of the industry, the sector risk, the transparency of blockchain technology, and the growing use of analytical tools to monitor for illicit activity. This would ensure that any AML/ATF obligations are proportionate to the risk of illicit activities using NFTs. We also encourage reviewing the approaches taken by FATF[20] or the European Union[21] to create a clear, harmonised legal framework.

    An AML/ATF framework for NFTs must be proportionate to the actual risk associated with the operations, products and services. The range of values of NFTs can vary from tens of dollars to millions. NFT service providers transact over recognized payment rails and work with regulated money services businesses around the world to provide users with wallets and other payment services. Requiring KYC information for all transactions would create an undue regulatory burden. There are a number of proportionate processes that could adequately mitigate fraud and illegal activities, such as geo-location, sanctioned country IP address blocking, collecting IPs addresses, transaction and fraud monitoring. Enhanced due diligence would be based on risk assessment of the clients, based on established risk guidance from FINTRAC.

    Prior to including NFTs under the PCMLTFA/R we encourage the government to assess those factors that indicate the relative risk of specific NFT platforms and services providers and work to ensure regulations are proportionate to such risks and involve clear definitions of the processes and providers they are meant to cover. These factors include (1) the level of criminal activity, (2) the size of transactions, and (3) defining the different activities of NFT service providers. **Our**

[19] Department of Finance Advisory Committee on Money Laundering and Terrorist Financing Link Here
[20] FATF "Money Laundering and Terrorist Financing in the Art and Antiquities Market", February 2023. Link here.
[21] European Parliament, "New EU Measures Against Money Laundering and Terrorist Financing", March 2023. Link here

members welcome the opportunity to share their technological expertise and experience with lawmakers.

26. Company Service Providers. Service providers cover a very broad range of activities and services and a distinction should be made between those that provide software as a service (SAAS) and more traditional services providers such as transfer agents and custodians. We do not generally agree that the AML/ATF regime be extended to company service providers such as transfer agents and custodians. Reporting entities that are also registered with a different regulator such as OSFI or a securities regulatory authority, have the obligation to ensure there are proper processes in place to oversee their service providers so that the regulated entity meets its own obligations. We view such an extension adding regulatory burden and costs with little added value.

27. To the extent that White Label Automated Teller Machines, including crypto ATMs are not part of a regulated entities business, we support bringing them into the AML/ATF regime as an MSB. However we note that obtaining “know your client” information may be difficult without partnering with a regulated entity. This may change as digital identities become commonplace.

28. Clarity around business relationships and when a registered/reporting entity is able to consider the relationship to have ended would be welcome in order to reduce regulatory burden. There is already a books and records requirement under the PCMLTFA/R and the closing of a business relationship, and related documents, should be consistent with the existing framework of maintaining the records for five years.

Chapter 8 - Regulatory Compliance Framework

29. We are supportive of a risk-based compliance oriented enforcement process for registrants and reporting entities. As part of terms and conditions for compliance failures, FINTRAC currently has the ability to require, under a compliance agreement, additional reviews/audits as necessary. As each situation is different, we do not believe it is necessary to mandate what elements should be covered by a compliance agreement.

30. We encourage FINTRAC to continue to apply a risk based mechanism when selecting registrants for review and the risk based framework should be developed in conjunction with other federal and provincial regulatory agencies to whom FINTRAC could delegate AML/ATF responsibilities. Clear guidance for compliance staff are critical to maintain cost-effective compliance programs that meet FINTRACs needs.

31. We do not believe it is necessary to specify the proficiency requirements for the chief anti-money laundering officer (CAMLO). Many of the reporting entities are regulated under another regulator such as OFSI, the securities regulatory authorities or other professional bodies, which have significant proficiency requirements. The PCMLTFA/R regulations already have a requirement for the CAMLO to be knowledgeable in the area of AML/ATF. The proficiency requirements also extends under securities regulation as AML/ATF are both business risks and reporting obligations for securities dealers. There are multiple ways of gaining this knowledge and experience, including domestic and international programs and training, and encourage the flexibility to

choose, especially as training may differ depending on the industry (e.g. virtual currency and VASPs).

32. We believe that any use of audio and video recording during compliance examinations should be at the discretion of the reporting entity or registrant as this could impact such matters as solicitor/client privilege.

33. The existing level of disclosure of violations and penalties imposed by FINTRAC provides sufficient detail for transparency to the public, industry and other regulators. FINTRAC could consider publishing findings of their compliance reviews and enforcement cases to provide industry with timely feedback and opportunities to learn from others. The existing administrative penalties against entities are sufficient to act as deterrents and punishment for non-compliance, without adding in administrative penalties against officers, directors or agents. We do support mechanisms such as credit for cooperation mechanisms to encourage cooperative and open communications with compliance and investigative staff.

34. Reporting Framework. We note that a recent technical update to FINTRAC caused significant issues for the industry, in terms of time, effort and cost. Remediation efforts due to the coming in force of rules prior to the technology being in place created an enormous amount of work for the industry, including remediation. We encourage FINTRAC to regularly survey reporting entities and registrants to understand any new or unresolved regulation implementation matters as well as technical issues.

35. Given the volume of transactions, the number of reporting entities and registrants and the lack of industry technology solutions, we do not support changes to the reporting timelines. Compliance resources are not unlimited and shortening timelines would create an undue burden, especially on SMEs.

36. Money Services Businesses and Foreign MSB Registration Framework. Working with other federal and provincial and territorial regulatory agencies to create a database of known unregistered or illegal entities operating in Canada could assist in identifying entities that should be registered as an MSB. Vetting MSB applicants to assess compliance readiness prior to registration takes time and additional resources by FINTRAC. There may be other ways using technology to ask questions to assess readiness as well as to have officers certify readiness. This could be used to identify those entities that are at higher risk of non-compliance and assess compliance readiness for those entities. Revoking registration for failure to comply must only be used after all other avenues are exhausted.

37. Universal registration for All Reporting Entities. We do not believe it is necessary for all reporting entities to be registered with FINTRAC. A number of the reporting entity categories are defined based on registration with another Canadian regulator such as OSFI, the securities regulatory authorities or a professional body, and where public registries exist. As noted above, reporting entities have similar obligations and are subject to FINTRAC compliance and enforcement as those that are required to be registered under the PCMLTFA/R.

We recommend that the PCMLTFA/R be reviewed and focus on the activities of reporting entities and registrants, rather on the category the entity falls within. For example, crypto trading platforms are registered as a MSB) with FINTRAC and as a restricted dealer under provincial and territorial securities laws. MSBs have travel rule requirements, are activity based and there are no monthly sanctions screening requirements. However, the crypto trading platforms are transitioning to registration as securities dealers under the Canadian Investment Regulatory Organization (CIRO). As a securities dealer, there are currently no travel rule requirements, all clients must be identified and the monitoring is focused at the account level These discrepancies result in crypto trading platforms being regulated as an MSB and as a securities dealer leading to confusion over when specific requirements apply, duplication of compliance efforts and regulatory burden. Focusing on the activities rather than the category of registration or reporting entity results in regulatory consistency, simplifies compliance and reduces regulatory burden

We note that most, if not all, regulators (such as OSFI and securities regulatory authorities) include AML as a business risk that the firm needs to and which is included in the compliance reviews by those regulators. We recommend the sharing of information between regulators of existing and new registrants, such as financial institutions or securities dealers, to gain a better understanding of the reporting entity population.

38. We fully support the use of short-term exemptive relief to allow for the testing of new technology and methods to comply with AML/ATF obligations. Similar "sandbox" mechanisms and innovation labs are used by securities regulators around the globe and have recently been adopted by OSFI.

39. De-risking. De-risking is a significant issue in Canada, and globally. All businesses and sectors are affected by de-risking by larger financial institutions. Entities in the digital asset space face sector bias and have particular difficulty in opening bank accounts with Canadian financial institutions or obtaining insurance from a Canadian provider. PEPs are also susceptible to de-risking not just in Canada but globally[22]. Without proper oversight and monitoring by government agencies (including the Department of Finance, FINTRAC and OSFI), the current prescribed AML/ATF risk-based approach encourages broad de-risking by FIs. The same will also be a challenge under the new Retail Payments Activities Act and regulations, which will just add more pressure to an existing problem that will continue to stifle innovation in the Fintech space if this is not resolved soon, in some equitable manner, for all involved.

    We welcome a study of the impact of de-risking activities by collecting empirical data of the extent and nature of client relationships being denied services or exited by certain reporting entities and registrants. This study should then be used to inform guidance on effective risk assessment and risk management practices. We encourage the Government of Canada to adopt measures that provide clarity to regulated entities on how to manage higher risk clients, without closing their accounts or denying services. This may also include a process for dispute resolution at the reporting entity/registrant level if an individual or entity has been de-risked. De-risking should be considered a last resort option by all registrants/reporting entities, in particular FIs.

[22] See Wall Street Journal "Nigel Farages Claim of Bank Account Closure Prompts UK Government Review", July 3, 2023 Link Here; BBC "Bank Account Closures Must be Fast Tracked, Says Minister", July 5, 2023 Link here.

Anecdotally, we understand that de-risking occurs to simplify processes and reduce costs of risk assessment, monitoring and investigation. All aspects of the financial/capital markets regulatory system need to work together to understand the economic impact of regulatory requirements such as risk-adjusted capital, reserve ratio for crypto assets (OSFI, OSC, CIRO). We note that de-risking impacts innovation and can stifle competition as it often targets SMEs who themselves may be reporting entities or registrants under the PCMLTFA/R. For example, in order to be registered in certain capacities (e.g. securities laws) you require a Canadian bank account and insurance from a Canadian provider. Compliance reviews undertaken by FINTRAC, OSFI and other regulators should assess the number of clients denied services or de-risked and assess the compliance program against these statistics, in particular to identify bias and sector targeting in their risk assessment, due diligence and monitoring processes.

40. Geographic and Sectoral Targeting Orders. We support the creation of a framework for Geographic and Sectoral Targeting Orders (GSTOs) similar to other global regulators. Timely information assists reporting entities and registrants with compliance by being able to focus resources on known higher risk areas. However, we urge caution against bias and being overly inclusive in reporting requirements when issuing GSTOs. Releasing the GSTOs in the Gazette as well as press releasing the adoption of new GSTOs would help with public outreach.

41. Source of Wealth/Funds Determination. We acknowledge other regulations, specifically certain elements of Canadian securities regulation, that requires registrants to validate sources of income/wealth[23] of an individual when conducting certain financial transactions (for example, accredited investors or eligible investors for exempt market transactions). However, we question the benefit to AML/ATF activities. In practice, it is very difficult to assess whether paperwork proving wealth is genuine. This is a problem for even experienced investigators due to the modern global nature of the economy and where fraudulent documents or references are commonplace. The regulatory burden is not only about time, but it also could have the unintended consequence of an increased risk of identity theft. We are not convinced that this would provide any serious benefit to fight financial crime. However, if this is eventually adopted, to reduce regulatory burden, we recommend that this control be implemented at the level of financial institutions, (FIs), not MSBs, as FIs are the primary sources of the money transferred to Canadian MSBs.

Chapter 9 – National and Economic Security

42. We agree that FINTRAC's mandate should be expanded to take a more proactive role in combating sanctions evasion as well as economic security or other threats to the security of Canada. We support centralising the collection of sanctions and TF reporting to facilitate the analysis of the information reported. Care should be taken in terms of limiting or prohibiting financial transactions. As noted above, de-risking is already an issue. It can also be very challenging to determine the use of funds in certain situations. As Canada, and other nations, move towards more open banking, implementing certain restrictions on transfers is challenging as technology is constantly changing and lags regulations.

[23] National Instrument 45-106 *Prospectus Exemptions*. See "Accredited Investor". Link here. See s.3.5 Companion Policy 45-106 *Prospectus Exemptions* Link here.

Conclusion

CW3 would like to thank the Government of Canada for the opportunity to comment. We and our members are available to provide additional context for our submission and/or to answer any remaining questions.

We recommend that the Government of Canada take a strategic and forward-looking approach to enhancing the current AML/ATF framework. We believe web3 technology creates opportunities for novel business models and for new market structures to evolve. In addition, the existing framework in the PCMLTFA/R may already support new technologies and services without significant amendments.

We see a need for more public consultations around possible new market structures and novel business models. We encourage open dialogue and collaboration to support innovation and to develop new/enhanced crypto asset policies and regulations that are strategic and forward looking, adaptable and fit for purpose. Given the intersections between crypto assets and traditional capital and financial markets and payment systems, we believe such consultations should include a broad cross section of participants in financial, capital and crypto markets and the public.

Working collaboratively, we can develop policy and regulations that strike the right balance between enabling economic and sector growth, while combating money laundering, terrorist financing and advancing Canada's security interests.

Yours truly,

The Canadian Web3 Council (CW3)

Canadian Web3 Council Members

Annex 1 – Technical Proposals

Proposal and Description	Considerations	Response
Record Keeping for Crowdfunding Platforms Align the record-keeping requirements for crowdfunding platforms with other reporting entities by requiring them to keep records of people who pledge $1,000 or more.	Would this requirement be commensurate to the potential risk posed by pledgers to crowdfunding platforms? Would it have a chilling or negative impact on pledges?	$1,000 is a very low limit. Not all crowdfunding activities have a criminal element. Currently the reportable threshold for financial institutions and other regulated entities under PCMLTFA/R is $10,000. We encourage applying a consistent approach across all platforms with a focus on higher quality of reporting rather than quantity.
Additional Beneficial Ownership Information Require reporting entities to collect the dates of birth and gender of beneficial owners.	Would reporting entities have challenges collecting this information?	As noted above, we support the creation of a centralised and secure beneficial ownership database, drawing on information obtained from provincial and federal government agencies,who should be tasked with the complete collection of all relevant information. Asking each registered entity to ask for the same information creates duplication, increases costs and slows processing times. However, we question the relevance of collecting gender information and more specifically, how that data point improves the effectiveness of the AML/ATF program. In general, we do not support the collection of unnecessary data as there are significant privacy and security considerations as the database will be used publicly.

Proposal and Description	Considerations	Response
Definition of Affiliated Entities Amend the definition of "affiliated entities" to include entities with combined financial statements, thereby allowing such entities to exchange information related to money laundering and terrorist financing.	How would this change impact reporting entities? Are there views on potential privacy considerations?	The expansion of the definition of "affiliated entities" to include non-registered entities is not encouraged. Where an industry is deemed to be a risk for ML/TF, the industry should be regulated and therefore the exchange of information should be permitted. There should be limits on the amount and type of information that can be shared. The sharing of non-public or personal information must be purposeful and reasonable, and should require the informed consent to sharing of information between entities.
Large Cash Transaction Reporting Exception Exempt the obligation to report large cash transactions to FINTRAC when an employee conducts the transaction on behalf of their employer.	Would this change create exploitable gaps or risks? The Department of Finance has heard this proposal from stakeholders and is seeking input to better understand the desired impact.	We support the exemption to report LCT when employees conduct the transaction on behalf of their employer. The employee conducting the transaction may change, there may be one or a few access/login points, thereby resulting in sharing of information, the employee may not be aware of the purpose of the transactions. We encourage the review of the use of this information by law enforcement as to whether the benefits outweigh the costs of the added volume of reporting.
Clarify the Notion of "Third Party" Align the distinct concepts of "third party" between the	The Department of Finance has heard this proposal from stakeholders and is	We support the use of common taxonomy across all aspects of the PCMLTFA/R. This is especially beneficial for smaller

Proposal and Description	Considerations	Response
requirements concerning large cash transaction reporting and account opening.	seeking input to better understand this proposal and its desired impact.	organisations, where individuals may perform a variety of functions. Different definitions for different activities create confusion, and result in errors and delays.
Authorized Signers on Business Accounts Remove the requirement to verify the identity of up to three authorized signers on a business account.	Would this change create exploitable gaps or risks? The Department of Finance has heard this proposal from stakeholders and is seeking input to better understand the desired impact.	There are challenges to keeping the authorised signers on a business account updated in general. Reporting entities and registrants should not be penalised when the owner of a business account does not communicate this information in a timely manner. Given the prevalence of digital signatures and logins, there could be exploitable risks if the business shares account login information.
Life Insurance Industry Exempt life insurance companies from having to verify the identity of a plan member's beneficiary in cases where the life insurance company was not required to verify the identity of the plan member. In cases where a life insurance company remitted funds or virtual currency to the beneficiary of an annuity or life insurance policy before verifying the identity of the beneficiary, require the life insurance company to take reasonable measures to verify the beneficiary's identity, and keep a record of the measures taken and whether they were successful.	Would these changes create exploitable gaps or risks? The Department of Finance is seeking input on the volume of electronic funds transfers performed by this sector.	We do not support this exemption. We believe the releasing entity should validate recipient information. Receiving entities should be able to rely on transfers/transactions from registered AML entities for ID verification. Placing the onus on downstream entities will only create friction and remove any benefits of real time settlement.

Proposal and Description	Considerations	Response
Consider removing or streamlining reporting obligations concerning electronic funds transfers for this sector.		
Provide Records to FINTRAC Promptly Require reporting entities to keep records in such a manner that they can be more promptly provided to FINTRAC than the current 30-day period.	Taking note of the FATF requirement for financial entities to be able to provide records to competent authorities "swiftly," what time period would be appropriate to specify for this requirement?	Investigations can take time and sometimes 30 days are required to complete investigations in order to complete the suspicious transaction report. Many registrants are small or medium size enterprises that do not necessarily have dedicated staff to perform AML reviews. Also, given the number of transactions that may occur, sorting through data takes time. As technology improves, in a cost effective manner, it may be possible to shorten time frames however not at this time.
Exceptions for Reporting Large Virtual Currency Transactions Consider adding exceptions for reporting virtual currency transactions of $10,000 or more to FINTRAC, considering that there are exceptions for reporting cash transactions of $10,000 or more.	What exceptions would be appropriate?	We encourage the consistent use of exceptions to reporting virtual currency transactions as for reporting cash transactions. We support the same exemptions.