

April 13, 2018

Director General  
Financial Systems Division  
Financial Sector Policy Branch  
Department of Finance Canada  
James Michael Flaherty Building  
90 Elgin Street  
Ottawa ON K1A 0G5

Via Email: [fin.fc-cf.fin@canada.ca](mailto:fin.fc-cf.fin@canada.ca)

**Re: Reviewing Canada's Anti-Money Laundering and Anti-Terrorist Financing Regime**

Dear Financial Sector Policy Branch:

[Organisation] is incorporated under the federal laws of Canada. [Organisation]'s primary business unit is [Organisation website], which serves as an online platform for customers to purchase Bitcoin (BTC), Bitcoin Cash (BCH), Ethereum (ETH), and Litecoin (LTC) which we resell from recognized operating exchanges in Canada. [Organisation] currently restricts its business dealings to Canadian residents and transacts exclusively in Canadian dollars with the provision that it cannot exchange currencies on behalf of any of its users.

[Organisation] welcomes the opportunity to provide comment on "Reviewing Canada's Anti-Money Laundering and Anti-Terrorist Financing Regime" as published February 7, 2018 by the Department of Finance Canada (the "Department") and consents in whole to the disclosure of this submission. In addition, [Organisation] requests that our identity and personal identifiers be removed prior to publication.

[Organisation] supports the Departments five-year mandate to review Canada's existing framework as established by the Proceeds of Crime (Money-Laundering) and Terrorist Financing Act ("PCMLTFA") that is "to keep the framework current in response to market developments as well as new and evolving risks<sup>1</sup>". [Organisation] has used this mandate to engage and educate senior management on existing and proposed efforts put forth by the Department to combat anti-money laundering ("AML") and anti-terrorist financing ("ATF").

*Digital ID*

[Organisation] agrees with the Departments assessment that since the last review, there is a need for modernized non-face-to-face identification measures. Key developments in the "Digital ID" era have been brought about by major advancements in digital identification technology and the growing use of mobile devices. These developments increasingly promote non-face-to-face interactions online and on mobile devices. The regulations surrounding non-face-to-face identification as defined in the PCMLTFR, although in line with Financial Action Task Force ("FATF") recommendations, have not kept up with "sophistication" used in financial crime, money laundering and terrorist financing.

---

<sup>1</sup> pg 5 - Reviewing Canada's Anti-Money Laundering and Anti-Terrorist Financing Regime  
<https://www.fin.gc.ca/activty/consult/amlatfr-rpcfat-eng.asp>

As an example, added measures could be taken to ensure that the identification methods used by Financial Transactions and Reports Analysis Centre (“FINTRAC”) are vetted at time of registration. This would be more inline with the licensing regimes in Europe (PSD) and the United States through FinCen (BSA). The “Customer Identification Process” that is being implemented by the regulated/licensed entity is reviewed as part of the overall Risk Based Approach to ensure it meets, and/or, exceeds the information requirements as prescribed by the regulator. Canada’s approach has been that entities register immediately, and then have the “Customer Identification Process” reviewed at the first examination. In most cases, this is two years or more from the date of the registered entity.

#### *Virtual Currencies*

**[Organisation]** recognizes the need to include Virtual Currencies within the fold of the PCMLTFA and believe that this is a necessary step towards the long-term viability of Virtual Currencies within the financial industry. Money laundering and terrorist financing threats will continue to exist so long as stricter guidelines are not imposed on businesses operating within the Virtual Currency landscape. Starting in 2018, **[Organisation]**, under the acknowledgement of Senior Management, has decided to be pre-emptive in creating a voluntary AML compliance regime within its **[Organisation]** ecosystem. The main objective of the AML regime will be to adhere to the Money Service Business (“MSB”) regulations as defined in the PCMLTFA. Knowing full well that this is not required, **[Organisation]** aims to be a leader in combatting money laundering and terrorist financing. While there is no shortage of reporting on fraudulent operators within the Virtual Currencies community, **[Organisation]** believes that there are other operators out there who similarly seek regulation as a framework for fighting money laundering and terrorist financing **[Organisation]** looks forward to the updated PCMLTFR that are to follow from the 2014 definition of Virtual Currencies.

#### *Undue Burden*

**[Organisation]** agrees that the result of this review should not create further “undue burden” and regulatory oversight and technological advances be adopted to better combat the proceeds of crime, money laundering and terrorist finance in Canada. Recommendations include, but are not limited to;

- Use of technologies to create not-for-profit consortium to enable “Zero-Knowledge Proof” result sets in identifying individuals. A good example is how the CRA is using SecureKey to authenticate end users through their online bank access.
- Centralized datastore to allow for the sharing of information across all sectors regulated by FINTRAC to combat PC/ML/TF. A good example of this is the Bank Crime Prevention and Investigation Office (BCPIO) as administered by the members of the Canadian Bankers Association (CBA). Although great care and forethought need to be taken into account to avoid Privacy Concerns.<sup>2</sup>
- We applaud the effort by DIACC<sup>3</sup> to standardize this for all Canadian individuals and corporations and suggest that a central registry for “Ultimate Beneficial Ownership” be created for Canada.

---

<sup>2</sup> Dec. 22/14 - PIPEDA Report of Findings #2014-018 <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2014/pipeda-2014-018/>

<sup>3</sup> Digital ID & Authentication Council of Canada - <https://diacc.ca/proofs-of-concept>

- Agree with the need to clarify section 7 & 8 of the Charter of Rights and Freedoms as it relates to various sections of the PCMLTFA to better define what would be considered in scope for ML/TF/PC as related to Solicitor-client privilege and the rule of law<sup>4</sup>.

#### Exchange of Information, Privacy, and Stronger Ties to Private Sector

Chapter Two identifies various initiatives and proposed changes to the acts to allow for increased flowing of information related to Proceeds of Crime, Money Laundering, and Terrorist Financing in both the private and public sector. **[Organisation]** believes these efforts will prove very helpful in combatting Proceeds of Crime, Money Laundering, and Terrorist Financing. There are reports daily of certain actors breaching Identity<sup>5</sup>, scamming and stealing funds<sup>6</sup>, and using the “dark web”<sup>7</sup> to conduct all sorts of illicit activities. As these efforts evolve, there is a growing need for Canadians to come together and combat the abuses in a more concerted effort both domestically and internationally<sup>8</sup>.

With respect to privacy, and as stated before, it would be in the best interests of all involved, consumers, businesses, and governments alike to begin adopting and implementing “Zero-knowledge proof”<sup>9</sup> systems that allow for data to be kept private while not allowing information to be breached. In this way, information can be checked but not leaked. And in the event further information is required by regulators or law enforcement, a special key or access route could be implemented to allow for deeper dives into the information.

#### Electronic Funds Transfers (“EFT”) over \$10,000

ISO 20022 which is being implemented by Payment Canada<sup>10</sup> for all EFTs in Canada includes the information disclosures necessary for FINTRAC. With respect to non-EFTs our view is that outside of mandatory reporting by regulated entities, this would be a hard gap to close. The regulated entities are not the problem in this situation. It is the ones that are operating illegally or under the radar that are more difficult to pin down.

#### De-Risking and Strengthening MSB Registration

**[Organisation]** agrees with the assessment that de-risking is a broad subject that crosses many businesses. Failure to address this any longer will make matters worse as companies will continue to obfuscate with their respective banks. This is happening with many lines of business, not just MSBs. The report seems to suggest that it’s really a problem with KYC, when in fact, the wholesale de-risking of entire categories of businesses has been happening for some time now as indicated in a report issued by

---

<sup>4</sup> Canada (Attorney General) v. Federation of Law Societies of Canada) - <https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/14639/index.do>

<sup>5</sup> Ontario man charged with selling billions of pieces of personal data through online site: RCMP - <https://globalnews.ca/news/3965405/ontario-man-charged-selling-personal-data-online-rcmp/>

<sup>6</sup> CRA scams on the rise as tax season gets underway - <http://www.cbc.ca/news/canada/ottawa/cra-scam-taxes-canada-1.4564308>

<sup>7</sup> Over 70,000 Canadian Credit Card Numbers Being Sold on the Dark Web - <https://darkwebnews.com/dark-web/70000-canadian-credit-card-sold-on-darkweb/>

<sup>8</sup> INTERPOL holds first DarkNet and Cryptocurrencies Working Group - <https://www.interpol.int/News-and-media/News/2018/N2018-022>

<sup>9</sup> Zero-knowledge proof - [https://en.wikipedia.org/wiki/Zero-knowledge\\_proof](https://en.wikipedia.org/wiki/Zero-knowledge_proof)

<sup>10</sup> Creating new opportunities in Canadian payments - <https://www.payments.ca/industry-info/modernization/iso-20022>

the FCA in the UK<sup>11</sup>. Another example is the memo that went out from Central 1 effective Feb. 28. 2018 which specifically restricts MSB's, FX Dealers, Casinos among others<sup>12</sup>.

If there were a counter-balanced approach here in Canada to enforcement similar to that of FinCen in the US where the Financial Institution must document the reasons for de-risking and/or not taking on the business in the first place, that would most likely be a good step. This worked somewhat effectively in the US and Europe. As Jamal El-Hindi Deputy Director at Fincen<sup>13</sup> state last year;

“MSBs play an important role in a transparent financial system, particularly because they often provide financial services to people less likely to use traditional banking services and because of their prominent role in providing remittance services, both domestically and abroad. FinCEN, as the agency primarily responsible for administering the Bank Secrecy Act (BSA), does not support the wholesale termination of MSB accounts without regard to the risks presented or the bank’s ability to manage the risk.”

### Conclusion

In conclusion, **[Organisation]** believes that matters within “Reviewing Canada's Anti-Money Laundering and Anti-Terrorist Financing Regime” can have real impact, especially with respect to Virtual Currency. When considering that the scope of this review will not be reviewed again for another five-years, it is important that these measures are dealt with now. The immediate impacts related to Digital-ID, Virtual Currency, and De-Risking should be dealt with swiftly as the current amount of undue regulatory burden is stifling innovation and competition in the Canadian marketplace.

**[Organisation]** supports the Departments decision to seek input from stakeholders as they aim to develop existing policy to combat Proceeds of Crime, Money Laundering and Terrorist Financing.

---

<sup>11</sup> FCA Research into the issue of de-risking - <https://www.fca.org.uk/news/news-stories/fca-research-issue-de-risking>

<sup>12</sup> PDF of memo is available upon request.

<sup>13</sup> <https://www.fincen.gov/sites/default/files/2016-09/20160606.pdf>