ELECTRONIC TRANSACTIONS ASSOCIATION

1620 L Street NW, Suite 1020
Washington, DC 20036

202.828.2635
electran.org

July 31, 2023

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

VIA E-MAIL: fcs-scf@fin.gc.ca

The Electronic Transactions Association (**ETA**) submits these comments in response to Finance Canada's consultation on strengthening Canada's anti-money laundering (AML) and anti-terrorist financing (ATF) regime. We hope that these comments offer the government more clarity on what kind of direction is required to develop a regulatory regime that is future-proof and well placed to deal with the complexities of a global financial ecosystem on the issues of AML/ATF.

ETA is the leading trade association for the payments industry, representing over 500 companies that offer electronic transaction processing products and services. ETA's members include financial institutions, mobile payment service providers, mobile wallet providers and non-bank online lenders that make commercial loans, primarily to small businesses, either directly or in partnership with other lenders. ETA member companies are creating innovative offerings in financial services, revolutionizing the way commerce is conducted with safe, convenient, and rewarding payment solutions and lending alternatives.

ETA appreciates the need for the government to conduct a Parliamentary Review of the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (PCMLTFA) and is delighted to offer its insights and expertise to support the government during this process. In our view, the proliferation of multiple innovative financial services, along with the ever-growing levels of financial connectedness between economies and individuals necessitates a dynamic approach to ensure that new financial models and relationships are captured under an AML/ATF regulatory regime.

Specifically, issues of how payment service providers (PSPs) and money service businesses (MSBs) are treated under the current framework when it comes to reporting, how the formatting and requirements for suspicious transaction reports (STR) can be improved are among some of the key concerns most relevant for ETA's members. Additionally, ETA is also supportive of the impending launch of the Canadian Financial Crimes Agency and believes that the centralization of reporting requirements when it comes to fraud should be a priority for the agency. These concerns are addressed in greater detail in the comments below.

## Building a culture of efficiency for the Canadian Financial Crimes Agency (CFCA)

ETA is supportive of the government's efforts to establish the CFCA as the lead enforcement agency for Canada in financial crime. As outlined in the consultation brief, a wide range of crimes and threats could be considered financial crimes, and ETA takes the view that various types of fraud, which may include securities and investment crimes, public corruption, and competition offences are suitable for inclusion in the CFCA's mandate.

Currently, there is a lack of clarity with regard to types of fraud-related transactions which are required to be reported as part of the suspicious transactions reporting requirement. This issue is further compounded by a wide variety of fraud-related transactions that go beyond the usual cases of cheque, internet, and wire fraud. Therefore, the absence of specific guidance could potentially lead to over-reporting or under-reporting by reporting entities. Additionally, the lack of a centralized reporting framework for reporting fraudulent transactions also introduces additional challenges as reporting entities are required to report all fraud related transactions to FINTRAC, while maintaining their reporting obligations to the Canadian Anti-Fraud Centre.

If the CFCA is to take the lead on all fraud investigations, reporting entities would benefit from having a clear definition of fraud related transactions that reporting entities are required to report, including some scenarios (based on data that is currently available to FINTRAC and similar to ML/TF indicators shared by FINTRAC) as well as clear guidance to help reporting entities better monitor, identify and report fraudulent transactions efficiently and effectively. We believe that such definitions should be heavily informed by fraud typologies, like what the Department of Justice Canada has done previously in 2002.[1]

ETA also believes that the CFCA should work closely with other federal and provincial money laundering (ML) /terrorist financing (TF) regulatory agencies to create a more centralized fraud reporting framework, which will serve as an information hub for these agencies to access data pertaining to fraudulent transactions as required.

The second issue when it comes to structuring the CFCA in a manner that enables more effective investigations relates to the introduction of a legislated “keep open” request. This could potentially pose additional operational and administrative challenges to reporting entities who have implemented policies to help mitigate ML/TF risks by filing suspicious transaction reports (STRs) and where applicable (based on the reporting entity’s risk appetite) close the account. If this “keep open” request is enforced, entities may be required to keep the account open pending a decision by law enforcement agencies or regulators on whether to close or keep the account open. There could also be potential delays in such a decision, given the current delay experienced with FINTRAC’s STR review/feedback at the moment. The institution would also need to deal with customer complaints and privacy requests (on a larger scale) due to potential restrictions that institutions would need to apply in order to keep accounts open.

If the CFCA is to be the lead agency for investigating STRs, ETA believes that the CFCA could achieve the same objective by providing clear guidance on types of cases that institutions should keep open when suspicious transactions are detected and reported, working in partnership with FINTRAC, law enforcement agencies and other regulators. This would help inform reporting entities policies and procedures around STR related follow-up actions.

**Public-to-Private Information Sharing: Database of Politically Exposed Persons (PEP) and Heads of International Organizations (HIO)**

Currently, the maintenance of databases of PEPs and HIOs is fragmented. Financial institutions often rely on lists from multiple private sources, and these could lead to inconsistencies and

[1] Department of Justice Canada (2002) A Typology of Profit-Driven Crimes. https://www.justice.gc.ca/eng/rp-pr/csj-sjc/crime/rr02_3/index.html.

sometimes inaccurate information on PEPs and HIOs. To this end, ETA would like to express its support for a government-led initiative to compile and maintain a centralized database of PEPs and HIOs, similar to what has been done with the Consolidated Canadian Autonomous Sanctions List.

## Scope and Obligations of AML/ATF Framework

### A Review of Existing Reporting Entities – Payment Service Providers (PSPs) and Money Services Businesses (MSBs)

ETA is concerned that an application of the same rules and obligations to PSPs and MSBs, which are materially different business types, could result in additional challenges and recommends that the government adopts a new approach to distinguish them under the PCMLTFA. Specifically, traditional MSBs offer products and services that have historically catered to a much smaller proportion of persons (those requiring foreign exchange or funds remittance across international borders), whereas payment service providers more broadly target persons conducting a wide variety of commercial activities.

As a result, PSPs typically have a much larger and more diverse client base than do traditional MSBs, and by extension, the number of transactions conducted by PSPs is much larger in comparison to traditional MSBs. Similarly, given that many PSP business models do not involve direct transmission of funds across international borders (e.g., traditional MSBs are often involved in the business of sending/receiving international wires to/from third-party beneficiaries), the relative money laundering/terrorist financing (ML/TF) risk presented by such PSPs is reduced. Some of our thoughts on what a new risk-based approach to regulating PSPs and MSBs should look like are outlined below for your reference:

#### *Create a category for PSPs as a reporting entity under the PCMLTFA*

In finetuning the government's approach to regulating PSPs and MSBs, ETA believes that PSPs should be defined as a reporting entity under the PCMLTFA. Currently, PSPs are primarily brought into scope as MSBs by nature of their remitting or transmitting funds by any means or through any person, entity, or electronic funds transfer network; and corresponding obligations (including those in respect of identity verification and recordkeeping) are expressed as a function of these activities.

As a practical matter, ETA's members take the view that it would be beneficial if the regulations defined both payment service provider and payment service provider services; and then framed corresponding obligations through the lens of these definitions. At a high-level, PSPs would benefit greatly if the regulations were cross-referenced against the typical lifecycle of a PSP transaction or PSP-merchant relationship to ensure the applicability of such regulations was made clearer and more direct, as opposed to depending upon the indirect application of funds remittance or funds transfer.

#### *Differentiated Client Identity Verification and Recordkeeping*

To strengthen the differentiation between PSPs and MSBs while ensuring that such a new approach is recognizant of the need to take a risk-based approach, ETA recommends that the

PCMLTFA applies differentiated identity verification and recordkeeping requirements for PSPs and MSBs.

By nature of the different products and services offered, the population of clients to which a PSP provides products and services is much larger than the typical MSB. What this means in real-life is individuals wishing to conduct commerce and participate in the Canadian economy are more dependent on having access to the products and services offered by a PSP than they are dependent on products and services offered by a traditional MSB, which also means that the ML/TF risks are different, as outlined in the preamble of this section.

In dealing with the different relative ML/TF risks presented by PSPs and traditional MSBs, ETA believes that it is not prudent to apply a set of common prescribed client identity verification methods across these different business types. ETA and its members hold the view that in order to ensure all persons have access to payment solutions, client identity verification methods prescribed should be specific to PSPs and exhibit a lower threshold than those applicable to MSBs. For example: the credit file method could be revised to allow for a shorter credit file history (e.g., one year instead of three). This is especially important within a not-in-person application context given a large proportion of PSPs lack in-person service delivery channels, and the majority of new clients are onboarded using not-in-person identity verification methods (e.g., these clients are onboarded using online platforms exclusively).

ETA is concerned that that the application of MSB-threshold identity verification methods exclusively has the unintended consequence of blocking access to the economy in respect of new immigrants or other foreign nationals who, although duly authorized to reside in Canada, and participate in economic activity in Canada, lack the credit history or other sources of information required under either the Credit File or Dual Process identity verification methods. While ETA recognizes that technologies to facilitate the Government-issued identification method for verifying identity on a not-in-person basis exist, such technologies are less successful when the identification presented is either issued by a foreign government or exists in the form of a Canadian Visa (IMM 1442 or equivalent).

As discussed above, if recordkeeping requirements were framed or qualified using payment card transactions or payment processing services (e.g., entering into an ongoing service agreement for the provision thereof), such an approach would make it easier to apply such recordkeeping requirements and avoid potential misinterpretation or other gaps.

Another point on identity verification and recordkeeping is raised via the nature of Service Agreement Records entered into with legal entities. Currently, MSBs are obligated to keep a record of the Name, Address and Date of Birth of each of the entity's employees who are authorized to order a transaction under the agreement. Within the context of PSPs, the number of employees contemplated by such recordkeeping is significantly higher than is the case with traditional MSBs, primarily due to the much larger size of the PSPs client population. Notwithstanding the fact that merchants are likely to have this information in their possession for employment-related purposes, requesting such detail presents an increasing privacy concern amongst Canadian merchants, which could lead to them being hesitant to share such information. Furthermore, such information does not need to be verified under the regulations, which brings further into question the need to collect such personal information to begin with. Therefore, ETA urges Finance Canada to consider refining the identity verification and recordkeeping requirements for PSPs.

ELECTRONIC TRANSACTIONS ASSOCIATION
1620 L Street NW, Suite 1020
Washington, DC 20036
202.828.2635
electran.org

**Regulatory Compliance Framework – Effective Oversight and Reporting Framework**

***Revise the reporting framework by expanding the values within Suspicious Transaction Reports***

As a final area of concern, ETA recommends that the government consider expanding the range of values within certain fields of the STR to support PSPs better with their reporting obligations with FINTRAC. Currently, the range of values available in certain fields within the STR do not lend themselves well to the types of transactions typically conducted by PSPs (credit/debit card or other payment card transactions). Consequently, the user is often required to select 'Other' and then describe accordingly in free-form text.

As an example, an ideal STR format that takes note of the above could look like this:

- Transaction>> Method of Transaction: should include Point of Sale Terminal
- Starting Action >> Type of funds: should include Payment Card (or Debit, Credit, Gift payment card)

To build on the above, PSPs also often have limited information in respect of Part E of the STR given this section corresponds to the Merchant's client (the cardholder/third party). As a result, the majority of these fields will remain blank; and ETA suggests that additional fields be added which are specific to credit/debit cards (e.g., card type, issuer). Additionally, certain fields within the STR exhibit character limitations which prevent the PSP from populating such fields with the most appropriate or practical unique identifier numbers (e.g., reporting entity report reference number)

As described earlier, the number of transactions processed by a PSP relative to a traditional MSB is on average significantly higher; this makes reporting transactions on an individual basis within the STR much more challenging - especially in consideration of their being a limit in respect of the number of transactions which can be included within a STR. Other jurisdictions (the United States and Europe), allow for transaction activity to be reported on an aggregated basis using CSV exports of transactional data - as opposed to populating a form with the details of each transaction, respectively.

In many instances, the nature of suspicion for a PSP arises at the Merchant level, as opposed to the cardholder/third-party level. Therefore, the ability to report transactions on an aggregated basis would not necessarily compromise the quality of financial intelligence included within the STR; and would further allow for the STR to be submitted to FINTRAC on an expedited basis. For example: if a Merchant conducted 500 transactions over a given time period that gave rise to suspicion, allow the PSP to report this activity in the aggregate within the STR itself, as opposed to having to report each transaction individually, and then provide for functionality that allows the PSP to upload a detailed CSV file which contains the details of each transaction contemplated in the STR (with formatted headers identifying what the data in each column represents).

If the proposed measures are adopted, ETA believes that this would help reduce the regulatory burden on industry without compromising on the need to collect accurate financial intelligence in a timely manner and submits our proposals on this matter for your consideration.

ELECTRONIC TRANSACTIONS ASSOCIATION

1620 L Street NW, Suite 1020
Washington, DC 20036

202.828.2635
electran.org

**Conclusion**

ETA thanks you for the opportunity to submit these comments to advance a more robust but well-calibrated regulatory framework to combat money laundering and terrorist financing. We would be pleased to discuss the comments herein with Finance Canada in greater detail and look forward to the revised PCMLTFA which plays a key role in safeguarding the integrity and resilience of Canada's financial industry.

Yours respectfully,

Scott Talbott
Senior Vice President
Electronic Transactions Association