TransferWise Canada Inc.
99 Bank Street, Suite 1420
Ottawa, ON K1P 1H4
www.transferwise.com
roseanne@transferwise.com

May 18, 2018

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

E-mail: fin.fc-cf.fin@canada.ca

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

Ladies and Gentlemen:

TransferWise understands that the Department of Finance Canada (the "**Department of Finance**") has requested comments on its paper "*Reviewing Canada's Anti-Money Laundering and Anti-Terrorist Financing Regime*" published on February 7, 2018 (the "**Review**"). TransferWise appreciates the opportunity to address certain issues discussed in the Review in order to improve the efficiency and effectiveness of Canada's anti-money laundering and anti-terrorist financing ("**AML/ATF**") regime.

Background

TransferWise is a financial technology company that was created in 2011 by Taavet Hinrikus, the first employee of Skype, and Kristo Käärmann, ex-Deloitte consulting, out of their personal frustration with unfairness in international money transmission. Since that time, TransferWise has raised more than $170 million from investors such as Andreessen Horowitz, Sir Richard Branson, and Peter Thiel, the co-founder of PayPal.

TransferWise addresses the challenges and costs associated with international money transmission — specifically the lack of transparency regarding fees and the calculation of foreign exchange rates — as well as the reliance on outmoded systems and technology. In response to these issues, TransferWise operates a robust international money transmission and prepaid account product that references fair exchange

rates, sources onshore liquidity when possible, provides a straightforward and transparent fee structure, uses modern technology, maintains sound customer service practices, and carefully manages liquidity, compliance and other risks.

Each month, the TransferWise group handles over $3 billion CAD equivalent in transaction volume for over 3 million customers worldwide, with approximately $330 million in monthly CAD volume alone. TransferWise Canada Inc. offers the service to Canadians and is registered with the Financial Transactions Reports Analysis Centre of Canada ("**FINTRAC**") with number M15193392 and has a license with the Quebec Autorite des Marches (number 902804).

Overview

TransferWise, as a global financial institution, understands the challenges associated with anti-money laundering and anti-terrorist financing and indeed spends significant resources to ensure not only compliance with applicable law, but also maintain appropriate practices geared toward preventing the use of its system as a vehicle for illegal activity of any kind.

Corporate Transparency

Like the Department of Finance, TransferWise recognizes that "corporate vehicles can be used to conceal the true ownership of assets" for illicit purposes and for this reason, and to comply with the Proceeds of Crime (Money Laundering) and Terrorist Financing Act ("**PCMLTFA**"), TransferWise takes steps to confirm the ultimate beneficial ownership ("**UBO**") structure of its business customers.[1] However, unlike other countries, as the Review points out, (*see* pages 18-19), Canada does not maintain a required centralised registry of beneficial ownership, making it difficult for financial companies to comply with PCMLTFA. We note the Finance Minister's agreement in principle, taken in December 2017, to amend the requirement that "corporations hold accurate and up to date information on beneficial owners that will be available to law enforcement, tax and other authorities,"[2] and would agree and argue that the Department of Finance needs to go further. Thus, we support the Department of Finance's determination that the lack of such a registry is a regulatory gap in Canada's AML/ ATF framework.

Guidance and rules regarding a central registry where UBO data must be reported and maintained by entities need to be promulgated and enforced. These should include a standardised format that entities must use for reporting and that financial companies can access. Without a requirement for entities to disclose this information in a standardised format to a registry, or simply to hold this information and ensure it is up to date and available, financial companies are left with few options and will struggle to take "reasonable measures" to confirm the accuracy of UBOs. Any enforcement of the requirement for financial companies to not simply collect information regarding UBOs, but to confirm the accuracy of this information, prior to the establishment of any requirement for entities to report this information to a central registry accessible by financial companies, would therefore be premature.

---

[1] *See*:
http://www.fintrac-canafe.gc.ca/guidance-directives/client-clientele/bor-eng.asp

[2] *See*: "Corporate Transparency" section at:
https://www.fin.gc.ca/activty/consult/amlatfr-rpcfat-eng.asp#Toc504749348

Politically Exposed Person ("PEP") Determination of Beneficial Owners

The PCMLTFA is also concerned with the identification of PEPs and the determination of whether they pose a risk of corruption, bribery or undue influence. In the case electronic funds transfers ("**EFT**") for more than $100,000, the PCMLTFA requires financial companies to have in place reasonable measures to determine whether a person involved is a PEP, or the head of an international organization, or a family member or close associate of any of these. Once positively determined, the financial company must then determine if the person poses a high risk for committing a money laundering or a terrorist activity financing offence. If assessed as such, then the person must be treated as a high-risk client.[3]

Given the importance of determining whether a customer may be exposed to the risk of corruption, bribery, or undue influence, we support the Department of Finance Canada's recommendations to require determination of whether UBOs are PEPs, and the application of prescribed measures to mitigate risks associated with PEPs.[4]

Engagement Model for Information Sharing with the Private Sector

Guidance, studies, trend reports, typology descriptions, and other information provided by FINTRAC regarding AML/ATF priorities could be useful in helping financial companies identify money laundering and terrorist financing risks. In addition, information such as examples of good and bad practices regarding effective risk management by financial companies, or frequently-issued typology descriptions, would strengthen the effectiveness of financial companies' understanding of AML/ATF risks and allow for development of more effective controls. For this reason, we support the Department of Finance's recommendation to establish a comprehensive information sharing framework between FINTRAC and the private sector.

Clarify the Electronic Funds Transfer ("EFT") or the "Travel Rule"

As indicated in the Review, the "travel rule" provides that financial companies must include with any EFT the name, address, and account number or other reference number of the client who requested the EFT, and that the financial company take reasonable measures to ensure that any transfer that the reporting entity receives includes this information.[5]

---

[3] *See:* FINTRAC guidance at:
http://www.fintrac-canafe.gc.ca/guidance-directives/client-clientele/Guide14/14-eng.asp

[4] *See:* "Expanding Requirements for Designated Non-Financial Businesses and Professions (DNFBPs) in relation to Politically Exposed Persons (PEPs), Head of International Organizations (HIOs) and Beneficial Ownership" section at:
https://www.fin.gc.ca/activty/consult/amlatfr-rpcfat-eng.asp#Toc504749348

[5] *See:* the "Clarify the Electronic Funds Transfer (EFT) or the "Travel Rule"' section at:
https://www.fin.gc.ca/activty/consult/amlatfr-rpcfat-eng.asp#Toc504749394

The Department of Finance's concern regarding industry implementation of the travel rule is justified, but with the emergence of fintech/new business models in Canada, including in the cross-border payments industry, this rule should be modernized. The rule should, for example, take into account that financial intermediaries do not always receive relevant information from originators or recipients. Information received depends on payment method (e.g., credit card versus EFT) and the financial companies involved.

In addition, the rule should be modernized to account for cross-border transfers. TransferWise, for example, seeks to avoid, for the benefit of customers, the costly and inefficient correspondent banking model. To do this, TransferWise partners with local banks around the world for payment accounts, so that payouts can be made on domestic rails. However, there remains an assumption in applicable rules that all cross-border payments use SWIFT or an equivalent system and exchange information in accordance with those system protocols. In the case of TransferWise, this is not the case, and domestic payments standards instead dictate what information it receives from the originating bank, and can therefore pass on. Domestic standards may be different from those in Canada, depending on jurisdiction, and may not support the inclusion of the information required by the travel rule. For example, the financial institution data that is provided to us often does not include elements like bank name, and bank identifier (e.g. IBAN, routing number, BIC).

This variation in domestic payments systems messaging standards presents difficulties for payment service providers (PSPs) and other intermediary financial institutions in their attempts to comply with the travel rule. Thus, without widespread, standardised adoption of the information required in the travel rule by countries worldwide, the effectiveness of the travel rule is diminished. There should be cooperation between domestic and international payment standards regarding adoption of such information.

Addressing the Issue of Money Services Business ("MSB") De-Risking

As the Review notes, de-risking is a real concern for MSBs operating in Canada, reflecting the perception that MSBs are high-risk and the mistaken belief in some cases that financial institutions must "know your customer's customer." *See* page 39. TransferWise agrees that MSBs need access to legitimate financial institutions, and for this reason, believes that FINTRAC should distinguish between different types of MSB business models. For example, some MSBs, like TransferWise, do not accept cash, and operate wholly online and without third party agents, which positively affects their risk profile. The lack of nuanced guidance for banks regarding different risk profiles of MSBs means that deserving MSBs are rejected when attempting to set up relationships to access payment account services, regardless of their risk profile.

While the Review acknowledges the adverse consequences of excluding MSBs from banking, including for financial inclusion, it remains the case that banks in Canada have the right to refuse to provide services to MSBs, and there are few if any protections in place to facilitate access to, or prevent the termination of, MSB payment account services. This issue could be addressed by following the EU model, where, for example, obligations have been imposed on member states to ensure that MSBs have access to credit institution (CI) payment account services on a 'objective, discriminatory and proportionate manner'.[6]

[6] *See:* Article 36, Revised Payment Service Directive at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L2366&from=EN

Many MSBs rely on access to payment systems via a banking partner in order to operate. Consequently, MSBs have to undergo lengthy processes in order to clear new and innovative product offerings with their partners (who are, in many cases, also their competitors). Banks may also refuse their services at any point, which can cause major disruption to MSB customers. It would be beneficial to MSBs, fintech companies, and consumers if a review of the conditions under which banks may terminate an existing relationships with MSBs were conducted. Creating more certainty around MSB banking relationships can contribute to a competitive and flourishing financial ecosystem by offering MSBs access to payment systems without undue hindrance. Anecdotally, we have heard both from both industry members and regulators in Europe that anti-money laundering concerns are often used to close down the account of MSBs by payment account providers, in order to terminate unprofitable business relationships.

Moreover, the only true way to create an fair and competitive playing field for financial companies is to provide direct access to domestic payment schemes for non-banks. There are few reasons to restrict direct access by appropriately licensed and audited firms, provided they can meet the requirements set out by the payment scheme, and do not pose any defined and specific settlement, operational or business risk.

Enhancing and Strengthening Identification Methods

Under the PCMLTFA, financial companies must identify customers using one of three different methods: (1) in-person, manual review of photo identification issued by the government; (2) the dual process method, requiring two original, current documents or information; or (3) the credit file method, using a credit file in existence for at least three years.[7]

The current regulatory framework is overly prescriptive in dictating how financial companies may identify customers, and, as mentioned in the Department of Finance's Review, does not allow for methods such as online validation of customer ID documents that could enhance the effectiveness of customer due diligence.[8] For this reason, TransferWise strongly supports the Department of Finance's observation that PCMLTFA Regulations should move toward adoption of new identification methods, including that "[r]egulations need to continue to remain flexible and adaptive in an environment of rapid development and emerging technologies" and that "more principles-based requirements could allow reporting entities to take a risk-based approach vis-à-vis new technologies."[9]

---

[7] *See:*
http://www.fintrac-canafe.gc.ca/guidance-directives/client-clientele/Guide11/11-eng.asp

[8] *See:* "Enhancing and Strengthening Identification Methods" section at:"
http://www.fintrac-canafe.gc.ca/guidance-directives/client-clientele/Guide11/11-eng.asp

[9] *See:* "Enhancing and Strengthening Identification Methods" sections at:
https://www.fin.gc.ca/activty/consult/amlatfr-rpcfat-eng.asp#Toc504749389

In-Person Review

For financial companies like TransferWise that offer services online only, in-person review of each customer's ID document is not feasible or scalable and would require a large network of agents or physical locations. Such an approach is incompatible with the online-only business model and indeed, as the Review notes, "the way people interact with and receive financial services has changed with the emergence of technologies that allow non-face-to-face interactions or foster an increasing array of complex financial products".[10]

Given the difficulties associated with in-person ID document review, online-only financial companies like TransferWise are required to choose either the dual process or credit file method method to identify customers.

Dual Process Method

The dual process method allows financial companies to use two original, valid and current documents or information from "independent and reliable sources" to identify customers.[11] The dual process method, however, does not give firms the option to use a copy or photograph of a government-issued photo ID document to identify customers remotely. This is not logical in that verification of the authenticity of the documents allowed for the dual process method, such as a utility bill or bank statement, is difficult. Unlike review of relatively standardised government-issued photo ID documents, variations in the myriad documents that fall under the dual process method make authentication of such documents challenging. Additionally, documents like bank statements are easier to forge than a government-issued ID.

Credit File Method

The credit file method allows financial companies to use a third party vendor for identity verification services. However, third party vendors offering credit file method services to financial companies have raised data protection concerns and limit how Canadian credit file information may be accessed, transferred, and stored. These concerns, in our experience, appear to have resulted in a reduced pool of providers, resulting in increased cost. We understand that the credit file method currently costs about $2 per credit file pull. This additional expense can present a barrier to entry for financial companies, who may not be able to afford the credit file identification method.

Moreover, the three-year minimum history of the credit file is discriminatory against both younger people, and potentially new migrants, who may not have an established credit history. TransferWise does not offer credit, and therefore this rule bears no reasonable relationship to the services sought. Thus, an

[10] *See:* "Key Developments Since the Last Review" section at:
https://www.fin.gc.ca/activty/consult/amlatfr-rpcfat-eng.asp#Toc504749382

[11] *See:*
http://www.fintrac-canafe.gc.ca/guidance-directives/client-clientele/Guide11/11-eng.asp

online identification method that does not require credit history should be available to financial companies, as outlined below.

Recommendation

Both the credit file and dual process methods illustrate the Government's willingness to embrace new technology, and allow flexibility in customer identification methods. However, a solution is needed that is scalable, affordable and digital.

Any change in the current PCMLTFA Regulations that would allow industry to make use of online validation of a government-issued photo ID document would be welcome and would address the issues raised above. Such a change would further reduce the risk of identity fraud, as a government-issued ID document is more difficult to forge than other documents currently used in the dual process method. Such a change would also bring Canada's customer identification framework for financial companies in line with those of other jurisdictions, such as the U.S. and the UK, where TransferWise already performs online validation of customer ID documents. Finally, online identification methods could include allowing financial companies to use additional tools, such as video identification of an individual customer alongside his or her ID document, to further minimise impersonation or identity fraud risk.

Consultation Process for the Development of Guidance

TransferWise would welcome any opportunity to engage with FINTRAC as it develops guidance regarding the PCMLTFA and Regulations, especially because such guidance is binding for financial companies. Industry engagement could allow FINTRAC to better understand how its guidance is implemented across financial companies, and identify any weaknesses in the guidance or opportunities for more efficient supervision.

As technology evolves increasingly quickly, it may become more important that FINTRAC has established a transparent relationship with industry so that it might benefit from private sector innovation. TransferWise welcomes any opportunity to constructively feed in to the guidance development process to help ensure the maintenance of an effective AML/ ATF regime in Canada.

Administrative Monetary Penalties ("AMP"): Public Naming

The AMP regime in the PCMLTFA sets forth the violations of the law and the prescribed range of penalty amounts for each violation.[12] In some cases, FINTRAC issues a notice of violation to financial companies that are found to be non-compliant, and applies corresponding penalty amounts to instances of non-compliance. Once all proceedings related to the violation are completed, FINTRAC may choose to make public the name of the person or entity and the violations and penalty amount imposed.

[12] *See:* Proceeds of Crime (Money Laundering) and Terrorist Financing Administrative Monetary Penalties Regulation at:
http://laws-lois.justice.gc.ca/eng/regulations/SOR-2007-292/page-1.html

Financial companies would benefit if the recipient of an AMP, along with the violation for which the AMP was issued, was publicly named by default.[13] Currently, a lack of transparency as to the kind of penalties issued, as well as a limited understanding of what constitutes a minor, serious, or very serious violation[14] undermines the efficacy of AMPs as a deterrent against violations of money laundering and terrorist financing rules. The ability for FINTRAC to withhold names of AMP recipient also presents the risk of inconsistent application of the AMP regulations. Without visibility into the enforcement decisions made by FINTRAC, financial companies have no means of determining whether the PCMLTFA and its regulations are enforced in a consistent manner.

Public naming of AMPs would also indicate to financial companies the priority level assigned by authorities to certain violations. Financial companies with knowledge of AMP recipients could, for example, align resourcing within the company to account for the priorities of national authorities and law enforcement. In addition, it is inefficient for the Department of Finance to enforce the law on a case by case basis, rather than in a public manner that allows financial companies to strengthen their understanding of law enforcement priorities. To the extent that the PCMLTFA requires financial companies to implement risk-based controls, information from government regarding violations of such requirements would provides feedback to industry on the law enforcement's perception of industry-wide risk.

For some violations, consumers may benefit from the public naming of AMP recipients, as individuals may have a higher likelihood of understanding a named financial company's past behaviour before entrusting the company with funds.

Confidentiality in Court Proceedings

As part of an AMP appeal process to a Federal Court, a financial company may apply to the court for a confidentiality order that could keep the identity of the violator confidential. We support the Department of Finance's view that the ability to apply for a confidentiality order "represents a significant departure from usual litigation processes in other spheres of federal regulatory compliance where the identity of regulated persons and entities is made public when the entities challenge a penalty that was imposed."[15]

---

[13] Although TransferWise supports public naming of AMP recipients by default, we support the Department of Finance's suggestion that "consideration should be given to criteria or situations when it would be appropriate not to name [AMP recipients], for example, when naming may affect the stability of Canada's financial system." *See*:
https://www.fin.gc.ca/activty/consult/amlatfr-rpcfat-eng.asp#Toc504749389

[14] *See:* Proceeds of Crime (Money Laundering) and Terrorist Financing Administrative Monetary Penalties Regulation at:
http://laws-lois.justice.gc.ca/eng/regulations/SOR-2007-292/page-1.html

[15] *See:* "Confidentiality in Court Proceedings" section at:
https://www.fin.gc.ca/activty/consult/amlatfr-rpcfat-eng.asp#Toc504749389

TransferWise supports publications of the final opinion of the appeal, along with the facts of the case. Publication of the final opinion would serve as an opportunity for clarification of the legislation or guidance in cases where ambiguity in the legislation, or in enforcement of the legislation, may have existed.

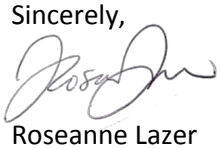
Finally, publication of the outcome of the appeal offers industry the opportunity to better adapt their controls to ensure compliance, and consumers the chance to understand past behaviour of financial companies, prior to investing, sending money or otherwise entrusting funds to the financial company.

* * *

We appreciate the opportunity to comment on the Department of Finance's Review of Canada's AML/ATF regime, and that the Department of Finance recognises the importance of continually evaluating the regime to address evolving money laundering and terrorist financing risks, while considering the needs of financial companies in Canada.

Please do not hesitate to contact us if you have any questions regarding this letter or if we can be of any assistance as you move forward.

Sincerely,



Roseanne Lazer
Compliance Officer, TransferWise Canada Inc.

CC:
Andrew Boyajan, Head of Banking, TransferWise Canada Inc.
Andrea Gildea, Head of Legal, TransferWise Canada Inc.
Antonio Occhiuto, Verification Team Lead, TransferWise Canada Inc.
Conor Danaher, License Program Coordinator, TransferWise Canada Inc.