Pay4B Limited

ANTI-MONEY LAUNDERING

&

COMBATING TERRORISM FINANCING

POLICY

Version 1.1

Pay4B Limited

Document Version Control – Pay4B Limited AML/CTF Policy

Revision Date	Document Owner	Version Number	Notes
10.03.2026	Company's Director Mr. Viktors Sereda	v.1.1	Incorporated effective Regulatory Amendments, made Business Risk Assessment

Pay4B Limited

Contents

1.1 INTRODUCTION

Company Registered Name	**Pay4B Limited**
Company Trading Name	**Pay4B**
Registered Business Address	Unit 807-130, Spadina Ave., Toronto, Ontario, M5V2L4, Canada
MSB Business Premises	Unit 807-130, Spadina Ave., Toronto, Ontario, M5V2L4, Canada
Registration/Authorization Details	Ontario Corporation Number 1000707154 and FINTRAC MSB registration No. N300000219 valid until 21st of September 2028 as well as registration No. under RPAA No. RPS0002997.
Company Director	Mr. Viktors Sereda
Ownership	Mr. Ihor Ustenko 100% ownership
Money Laundering Reporting Officer	Email: v.sereda@pay4b.com/legal@pay4b.com/ m.hryf@pay4b.com Contact No + 1 (416) 474 37 58
Contact Details	Main Office Telephone: + 1 (416) 474 37 58 Main Office Fax: NA Email ID: v.sereda@pay4b.com/legal@pay4b.com/ m.hryf@pay4b.com General email: v.sereda@pay4b.com/legal@pay4b.com/info@pay4b.com

Pay4B Limited will hereinafter be referred to as the "Company".

Purpose of this **Pay4B Limited** AML/CTF Compliance Manual (hereinafter referred to as the **"Manual"**) is to set forth **Pay4B Limited** procedures to Combat Money Laundering and Terrorist Financing (hereinafter collectively referred as AML/CTF) in accordance with Applicable Regulations. **Pay4B Limited** offers Remittance & Foreign Exchange Services, to the public through the network of agents, Authorized Partners/Money Transfer Operators, through company-owned Branches and Via Web based Services.

If you are an Agent/Partner of the Company, you have executed an agreement with the Company governing the provision of money transfer services (**Money Service Business or MSB**) and setting forth each party's obligations. As

part of your obligation to the Company under your agreement, you are required to take note of and at all times abide by the provisions of the Manual.

Failure to do so:

- Is considered by the Company to amount to a breach of your agreement, and may result in the Company terminating its agreement with you; and

- In certain cases may amount to breach of applicable legislations, which may result in civil and/or criminal penalties against you.

If you are an employee of the Company, you are required to take note of and at all times abide by the provisions of the Manual. Failure to do so:

- Is considered by the Company to amount to a breach of your duty as an employee, and may result in the Company terminating your employment with the company; whether for just cause (serious misconduct) or for termination of contract; and

- In certain cases may amount to breach of applicable laws, which may result in civil and/or criminal penalties against you.

This Manual is kept under periodical review by the Company, and you may from time to time be notified of revisions to its terms.

Please ensure that all of your staff involved in Money Service Business are familiar with the terms of this Manual and acknowledge this by executing and returning an executed acknowledgement in the form in Appendix VI.

Money Service Business are subject to strict laws and regulations designed to prevent Money Laundering/ Terrorist Financing and to bring those engaged in these illegal activities to justice. Failure to follow these laws and regulations can result in severe civil and/or criminal penalties including fines and imprisonment. The Company has established strict standards of compliance with all Applicable laws and regulations and is committed for the eradication of Money Laundering & Terrorist Financing which are summarised in this Manual. The purpose of the Manual is to explain in simple terms to Agents, Affiliated Partners and their staff and to the Company's Senior Management and Employees how to follow the applicable laws and regulations. If you are an Agent/Affiliated Partner, you are instructed to ensure that each of your staff reads this Manual carefully and completely, and to direct any questions they may have from time to time in the first instance to our Compliance Department.

2.1 SENIOR MANAGEMENT DECLARATION

Date: 10th of March 2026

I, the undersigned, being the Director of Pay4B Limited hereby endorse the policies which have been set down in this Compliance Policy Manual.

The manual covers the following areas:

- Money Laundering & Terrorist Financing Risk to our Business
- Measures we took to mitigate identified Risks
- Customer Due Diligence
- Training and Record keeping
- Suspicious Activity Reporting

These policies may be subject to amendment or addition as required for legislative and business operational reasons.

I confirm that it is the responsibility of the Money Laundering Reporting Officer (MLRO) to monitor Compliance with all of the policy issues mentioned above.

As and when required, the MLRO will make a report to senior management about any operational or strategic issues for the company which arises as a result of the policies set down in this manual.

We also confirm that it is our company policy that all members of staff (and agents, if applicable) must read and confirm in writing their understanding of the policies set down here – and their personal responsibilities arising for them.

In the event that staff members fail to comply as required with the policies in this manual, this will be regarded as a material breach in contractual obligations and may lead to disciplinary proceedings.

Signed by:

Mr. Viktors Sereda (CEO)

3.1 MONEY LAUNDERING

The Money Laundering Regulations require a fundamental understanding of the processes that can be involved in money laundering and require that you respond appropriately to any knowledge or suspicions that these processes may be taking place. This section of the policy explains what money laundering is, the offences and the penalties.

The term “money laundering” (ML) is defined in section 1 of Part 1 of Schedule 1 to the AMLO and means an act intended to have the effect of making any property:

(a) that is the proceeds obtained from the commission of an indictable offence under the laws and regulations of Canada, or of any conduct which if it had occurred in Canada would constitute an indictable offence under the laws and regulations of Canada; or

(b) that in whole or in part, directly or indirectly, represents such proceeds,

not to appear to be or so represent such proceeds and given the appearance of being legitimate by being exchanged for ‘clean’ money. Participating in the handling of such funds is illegal, and it can also be illegal to become involved in them with knowledge or suspicion.

There are three common stages in the laundering of money, and they frequently involve numerous transactions. An MSB provider should be alert to any such sign for potential criminal activities. These stages are:

Placement: the physical disposal of money remiitance in SEPA / SWIFT proceeds derived from illegal activities which means after a crime has been committed, funds are paid into a bank account or used to buy an asset.

Layering: separating illicit proceeds from their source by creating complex layers of financial transactions designed to disguise the source of the money, subvert the audit trail and provide anonymity or in other words to try and hide the source of the proceeds of crime, criminals carry out transactions, which can be complex and numerous.

Integration: creating the impression of apparent legitimacy to criminally derived wealth. In situations where the layering process succeeds, integration schemes effectively return the laundered proceeds back into the general financial system and the proceeds appear to be the result of, or connected to, legitimate business activities, meaning once the origin of the funds has been hidden through sufficient 'layering', the funds are imported back into the financial system.

Being involved in any of these three stages is potentially a criminal activity.

4.1 TERRORIST FINANCING

The term “terrorist financing” (TF) is defined in section 1 of Part 1 of Schedule 1 to the AMLO and means:

A. the provision or collection, by any means, directly or indirectly, of any property –
   I. with the intention that the property, be used; or
   II. knowing that the property will be used, in whole or in part, to commit one or more terrorist acts (whether or not the property is actually so used);

B. the making available of any property or financial (or related) services, by any means, directly or indirectly, to or for the benefit of a person knowing that, or being reckless as to whether, the person is a terrorist or terrorist associate; or

C. the collection of property or solicitation of financial (or related) services, by any means, directly or indirectly, for the benefit of a person knowing that, or being reckless as to whether, the person is a terrorist or terrorist associate.

Terrorists or terrorist organizations require financial support in order to achieve their aims. There is often a need for them to obscure or disguise links between them and their funding sources. It follows then that terrorist groups must similarly find ways to launder funds, regardless of whether the funds are from a legitimate or illegitimate source, in order to be able to use them without attracting the attention of the authorities.

5.1 Pay4B Limited AML/CTF POLICIES AND PROGRAM

Pay4B Limited takes all reasonable measures to ensure that proper safeguards exist to mitigate the risks of Money Laundering (ML) and Terrorist Financing (TF) and to prevent a contravention of any requirement under the Anti-Money Laundering and Counter-Terrorist Financing (Financial Institutions) Ordinance, Chapter 615, Laws and regulations of Canada (AMLO) and the related Guideline on Anti-Money Laundering and Counter-Terrorist Financing (AML Guideline).

Pay4B Limited establishes and implements adequate and appropriate Anti-Money Laundering (AML) and Counter-Terrorist Financing (CFT) policies, procedures and controls taking into account factors including types of customers, products and services offered, delivery channels and geographical locations involved.

Pay4B Limited and its directors and senior management are committed to operating the business in a transparent and open manner that is consistent with regulatory obligations. The directors, senior management, compliance officer and the nominated officer (MLRO) will always ensure that all suspicious activity is reported to the relevant authorities. It is our policy that commercial considerations shall never take precedence over our AML and CFT commitments.

As part of this commitment, **Pay4B Limited** will adopt strict procedures to comply with all applicable AML and CFT rules and regulations. Specific emphasis will be made on the main pieces of legislation in Canada that are concerned with Money Laundering (“ML”), Terrorism Financing (“TF”) and financial sanctions: the Anti-Money Laundering and Counter-Terrorist Act, The Proceeds of Crime (Money Laundering) and Terrorist Financing Act ("PCMLTFA"), the Controlled Drugs and Substances Act (CDSA), the Criminal Code of Canada, section 467, section 231 and the other relevant laws and regulations, existing in Canada for the purpose of avoidance and combat with businesses, involved in money laundering schemes, the United Nations (Anti-Terrorism Measures) Ordinance, Cap. 575 (UNATMO), the United Nations Sanctions Ordinance, Cap. 537 (UNSO) and the Weapons of Mass Destruction (Control of Provision of Services) Ordinance, Cap. 526 (WMD (CPS)O) and FATF Recommendations.

To comply with the listed regulations is extremely important for the Company as the AMLO makes it a criminal offence if an MSB (1) knowingly; or (2) with the intent to defraud the Commissioner of the FINTRAC and Bank of Canada regulatory authorities, contravenes a specified provision of the AMLO. The “specified provisions” are listed in section 5(11) of the AMLO. If the MSB provider in Canada knowingly contravenes a specified provision, it is liable to a maximum term of imprisonment of 2 years and a fine of $1 million upon conviction. If the MSB provider in Canada, contravenes a specified provision with the intent to defraud the CCE, it is liable to a maximum term of imprisonment of 7 years and a fine of $1 million CAD upon conviction.

Provisions of the Personal Information Protection and Electronic Documents Act 2000 (PIPEDA), effective since January 1st 2004 governs the processing relating to individuals, including obtaining, holding, use of disclosure of information.

Proof of Funds

Bank statement - in name of the customer and the amount sent cannot be deposited in the same day into customer account. Bank statement will be accepted just for amounts that meet the income of the customer.

- Saving account
- Loan agreement - note that with loan agreement customers shall demonstrate the amount come into their account.
- Funds from other person: Beneficial owner need to be identified and proof of funds should apply for the beneficial owner instead of the customer.
- Proof of address (domicile): Utility bill (gas, electricity, landline, bank statement), Canadian driving license and/or national ID card (if it is not use as proof of ID).

IMPORTANT NOTES:

Please note that currently we are not requesting proof of address, however it might be requested if the information provided is mismatch or incomplete.

The thresholds listed above is just a reference and the amounts are set up in our operational system. However, compliance department can stop any transaction and request further documents regardless the amount. Transactions placed with amount right below the limit set up above will be treated as unusual transactions and further action will be taken.

Deposits in money remiitance in SEPA / SWIFT into our account will be considered "non-face to face" transactions in money remiitance in SEPA / SWIFT and ID will be required for any amount. The thresholds applied will be the same applied to money remiitance in SEPA / SWIFT transactions.

Aggregate in a year CAD $120,000 - proof of occupation will be required. In some cases, if it's a single transaction more than CAD $120,000, proof of funds + proof of occupation will be required.

Compliance form is available in Appendix III.

6.1 LINKED TRANSACTIONS

Linked transactions may be a series of transactions by a legitimate customer, or they may be transactions that appear to be independent but are in fact split into two or more transactions to avoid detection.

Simply put, a client may attempt to disguise a remittance payment by breaking it into several smaller sums and utilizing his/her friends or family to send the funds usually to a single beneficiary.

In anticipation that a client will avoid requiring proof of funds and have structured his/her transactions in reaching the limit amount, the client may divide the amount among his/her friends and send the money at the same time to a single beneficiary. In this case, our remittance front-end IT system is a valuable asset as it will assist towards detecting linked transactions.

Staff must exercise personal judgment and consider the following:

- Are a number of transactions carried out by the same customer within a short space of time?

- Could a number of customers be carrying out transactions on behalf of the same individual or group of individuals?

- In the case of money transmission, are a number of customers sending payments to the same individual?

In the event that 'linked' transactions are identified, they should be notified to the MLRO who will determine whether or not there are any suspicious circumstances and whether the transaction should be reported to JFIU.

6.2 POLITICAL EXPOSED PERSONS - PEPs

One of the most prominent risks to the financial services sector is the risk posed by public officials, their associates and family members. There have been a number of damaging high-profile money laundering scandals within the private banking sector that have involved PEPs

A domestic PEP is defined as:

a) an individual who is or has been entrusted with a prominent public function in a place within the People's Republic of China and
I. includes a head of state, head of government, senior politician, senior government, judicial or military official, senior executive of a state-owned corporation and an important political party official;
II. but does not include a middle-ranking or more junior official of any of the categories mentioned in subparagraph
b) a spouse, a partner, a child or a parent of an individual falling within paragraph (a) above, or a spouse or a partner of a child of such an individual; or
c) a close associate of an individual falling within paragraph (a).

A (foreign) PEP is defined in the AMLO as:

a) an individual who is or has been entrusted with a prominent public function in a place outside the Canada and
I. includes a head of state, head of government, senior politician, senior government, judicial or military official, senior executive of a state-owned corporation and an important political party official;
II. but does not include a middle-ranking or more junior official of any of the categories mentioned in subparagraph
b) a spouse, a partner, a child or a parent of an individual falling within paragraph (a) above, or a spouse or a partner of a child of such an individual; or
c) a close associate of an individual falling within paragraph (a).

The AMLO defines a close associate as:

a) an individual who has close business relations with a person falling under previous paragraph above, including an individual who is a beneficial owner of a legal person or trust of which the person falling under paragraph above is also a beneficial owner; or
b) an individual who is the beneficial owner of a legal person or trust that is set up for the benefit of a person falling under paragraph above.

EDD in respect of PEPs shall be:

Having appropriate risk-sensitive procedures, known to all Employees and agents, to determine whether the customer or the ultimate beneficial owner is a PEP residing in a foreign country. Such procedures involve assessing the

information provided by the customer, publicly available information, or information contained on commercial databases relating to PEPs.

Obtaining prior approval from the Compliance Officer before entering into a business relationship with a PEP or executing an occasional transaction for a PEP.

Taking adequate measures to establish the source of wealth and source of funds that are involved in the business relationship or transaction. Employees should also, on a risk-sensitive basis, verify the source of funds and require documentary evidence; and

Conducting enhanced ongoing monitoring of the business relationship.

When dealing with clients with a more sophisticated financial profile, we should search about the provenance of their wealth such as: where their net worth was originally earned or acquired and the origins of their income;

The usual origins of wealth and income for PEPs might include:

- Business activity including business disposals, to determine whether the magnitude of their business activity is consistent with the wealth and income claimed.

- Employment: inquiries about salary, bonuses, share options to determine whether their employment is capable of generating the accumulated wealth.

- Investments: we will ask about the origin of the funds that purchased the investments in the first place. We will search for the magnitude and nature of the investments, annual income and capital growth, to determine whether the client's holdings are consistent with the wealth and income declared.

- Family money: we will search about the original source of the wealth, who transferred it to the client, when and in what form, and how that person earned or acquired the wealth, to determine whether inheritance provides a satisfactory explanation for the wealth and income claimed.

The requirement to identify close associates of prominent public functionaries as PEPs only applies to the extent that the relationship is publicly known or that the Company has reasons to believe that such a relationship exists. Thus it does not presuppose active research on the Company's part.

PEPs do not normally include public functionaries at regional or local levels of government. However, where their political exposure is comparable to that of similar positions at national level, the Company will assess, on a risk-sensitive basis, whether those persons should be considered PEPs.

The Company, its Employees and, in particular, the Compliance Officer must closely monitor all ongoing business relationships with PEPs.

All transactions will be screened against PEP lists, and any transactions with possible PEP matches will be stopped by our system for further analysis. Confirming PEP status or otherwise may require us to gather more information about the customer. The information that we will request is date of birth (DOB), place of birth and proof of occupation. This information will be used to compare and confirm if the client is a PEP or not.

If we confirm that the customer is a PEP, we will make sure that the correct profession is allocated in our system to meet the customer risk criteria.

7.1 TRANSACTION MONITORING

The Company monitors all transactions generated on its system to ensure compliance with the AML Manual, applicable legal and regulatory requirements by way of a two-level approach:

First Level

The Company adopts a hybrid model for monitoring its transactions. This includes a combination of automated and manual processes. All transactions undergo a stringent compliance process that includes:

- Sanctions & PEP Screening: The Company performs sanctions screening against the sanctions and PEP database maintained in in-house system. Alerts are investigated and closed as per the procedures set in this regard.

- Real Time Transaction Monitoring: Based on various rules, and defined thresholds and velocity controls, transactions undergo automated surveillance. The Company has an in- house developed surveillance system that has embedded the required rules. The compliance department undertakes the initial review and investigation. Transactions are assessed for (among other things) conformity with the Company's policy, data quality, structuring effort and restrictions on high-risk country involvement and, where applicable thresholds are met, the provision of supporting evidence (e.g. of the source of funds). The Company's MLRO conducts further investigation of any transaction that is flagged on the basis of this screening and determines whether any further action is required including, for example an SAR submission.

- Specific Post Facto Analysis: The compliance department of the Company along with assistance of a dedicated back-office unit, conducts periodic analysis on agents and their transactions. The reports and the findings are submitted to the MLRO so that appropriate actions are undertaken. The analysis looks for specific patterns, unusual patterns, data quality standards, and similar warning flags.

Second Level

This monitoring is a more detailed risk-based assessment of agents' activities. This is carried out by the compliance department of the Company along with the assistance of a dedicated back-office unit. Sample data sets for agents (selected on the basis of risk) are extracted from the Company's system and a shadow CDD exercise is undertaken. In the event of any concerns as to the adequacy of process followed by an agent, the Company's MLRO approaches the agent for clarification. Periodic compliance visits to agents will be carried out in person to discuss any major or recurrent issues that have arisen through the monitoring process, as well as to check record keeping, training and to discuss the overall risk and compliance environment. The frequency of visits to an agent is determined by Agent's risk classification.

8.1 SUSPICIOUS ACTIVITY REPORTING

What is Suspicious Activity:

"Suspicious activity" is a difficult concept to define because it can vary from one transaction to another based upon on all of the circumstances surrounding the transaction, or group of transactions. However in general suspicious Activities/transactions refers to any transaction or group of transactions about which doubts arise with the registered person concerning their link to money laundering and terrorist financing through their unusual size, repetition, nature, conditions and circumstances surrounding them, their unusual pattern that does not involve a clear economic objective or an obvious legal purpose, if the activities of the persons involved in the transaction(s) do not conform with their normal activities. For example, transactions by one customer may be normal because of your knowledge of that customer, while similar transactions by another customer may be suspicious.

In brief, the factors involved in determining whether transactions are suspicious, including the amount, the location of your business, comments made by your customer, the customer's behavior etc. A good rule to follow is that if a transaction is inconsistent with the business or personal circumstances of a customer and there is no reasonable explanation for the inconsistency, then it may be suspicious. Just because a customer appears on the suspect list it does not mean that he/she is involved in illegal activity. It only means that such transaction requires closer scrutiny.

What is Suspicious Activity Reporting:

The Suspicious Activity Report is a tool for identifying and reporting transactions that could be related to money laundering or terrorist financing. You need to refer any transactions you consider suspicious to the Company by:

- Completing a Suspicious Activity Report Manual/Electronic form for any transaction or pattern of transactions – completed or attempted – that is suspicious.

- Faxing the completed Manual form to the Company or to your local Regulator if required by law as soon as the suspicious activity is discovered

8.2 RECEIVING & REPORTING SAR – CORE OBLIGATIONS

The AMLO guidance explains the core obligations of receiving and reporting of suspicious activity

- All staff must raise an internal report where they have knowledge or suspicion, or where there are reasonable grounds for having knowledge or suspicion, that another person is engaged in money laundering, or that terrorist property exists
- The firm's nominated officer (or their appointed alternate) must consider all internal reports
- The firm's nominated officer (or their appointed alternate) must make an external report to the FINTRAC (FINTRAC) as soon as is practicable if he considers that there is knowledge, suspicion, or reasonable grounds for knowledge or suspicion, that another person is engaged in money laundering, or that terrorist property exists
- The firm must seek consent from the FINTRAC before proceeding with a suspicious Activity/transaction or entering into arrangements
- Firms must freeze funds if a customer is identified as being on the Sanction List of suspected terrorists or sanctioned individuals and entities, and make an external report to FINTRAC
- It is a criminal offence for anyone, following a disclosure to a nominated officer or to the FINTRAC, to do or say anything that might either 'tip off' another person that a disclosure has been made or prejudice an investigation
- The firm's nominated officer (or their appointed alternate) must report suspicious approaches, even if no transaction takes place
- Actions required, to be kept under regular review
- Enquiries made in respect of disclosures must be documented
- The reasons why a Suspicious Activity Report (SAR) was, or was not, submitted should be recorded
- Any communications made with or received from the authorities, including the FINTRAC, in relation to a SAR should be maintained on file
- In cases where advance notice of a transaction or of arrangements is given, the need for prior consent before it is allowed to proceed should be considered

Persons in the regulated sector are required to make a report in respect of information that comes to them within the course of a business in the regulated sector:

- where they know or
- where they suspect or
- where they have reasonable grounds for knowing or suspecting

That a person is engaged in, or attempting, money laundering or terrorist financing. Within this guidance, the above obligations are collectively referred to as "grounds for knowledge or suspicion".

8.3 SUSPICIOUS INDICATORS

The following lists are provided for staff as an aid to whether a particular transaction may be suspicious. The list is not limited to and staff & Agents should consider all the circumstances of a particular transaction before deciding whether to report any issues to the MLRO.

New customers and occasional or “one-off” transactions:

- Checking identity is proving difficult.
- The customer is reluctant to provide details of their identity.
- There is no genuine reason for the customer using the services of an MSB provider
- A money remiitance in SEPA / SWIFT transaction is unusually large.
- The money remiitance in SEPA / SWIFT is in used notes and/or small denominations.
- The customer requests currency in large denomination notes.
- The customer will not disclose the source of money remiitance in SEPA / SWIFT .
- The explanation for the business and/or the amounts involved is not credible.
- A series of transactions are structured just below the regulatory threshold for due diligence identity checks.
- The customer has made an unusual request for collection or delivery.
- Transactions having no apparent purpose, or which make no obvious financial sense, or which seem to involve unnecessary complexity.
- Unnecessary routing of funds through third parties.

For Regular and established customers.

- The transaction is different from the normal business of the customer.
- The size of frequency of the transaction is not consistent with the normal activities of the customer.
- The pattern of transactions has changed since the business relationship was established.
- Money transfers to high-risk jurisdictions without reasonable explanation, which are not consistent with the customer’s usual foreign business dealings.
- Sudden increases in the frequency/value of transactions of a particular customer without reasonable explanation.
- Examples where customer identification issues have potential to indicate suspicious activity.
- The customer refuses or appears reluctant to provide information requested.
- There appears to be inconsistencies in the information provided by the customer.
- The customer’s area of residence is inconsistent with other profile details such as employment.
- An address appears vague or unusual.
- The supporting documentation does not add validity to the other information provided by the customer.
- The customer is in a hurry to rush a transaction through, with promises to provide the information later.

Examples of activity that might suggest to staff that there could be potential terrorist activity:

- The customer is unable to satisfactorily explain the source of income.

- Frequent address changes.
- Media reports on suspected or arrested terrorists or groups.

8.4 PROCEDURE FOR REPORTING SUSPICIOUS CIRCUMSTANCES

Any member of staff or agent, who is suspicious that a transaction may involve money laundering or who becomes aware in the course of their work that someone else is involved in money laundering, must make a disclosure to the MLRO using the report form, by mean of email or using system.

Upon receipt of the Internal SAR by the MLRO, he will then decide what is to be done as a result of the report, e.g., whether the matter must be reported to the FINTRAC and to Bank of Canada or not, or further enquiries made and record its decision and the reason for it on the report form on the Database. The member of staff concerned must be informed of the decision and the reasons for it.

If the matter is referred to the FINTRAC and Bank of Canada the MLRO or his deputy will be responsible for completing the FINTRAC and Bank of Canada report form and discussing with the reporting member of staff how matters with the client/transaction are to be conducted from that stage.

In accordance with the tipping off provisions, the report must not be discussed with the customer.

Suspicious Activity/transaction reports can be made to JFIU in one of the following ways:

- by e-reporting system_____
- by email to _____
- by fax to: + 1 (416) 474 37 58
- by mail, addressed to FINTRAC, _____
- by telephone + 1 (416) 474 37 58 (for urgent reports during office hours)

The FINTRAC and Bank of Canada will acknowledge receipt of an SAR made by an MSB provider under relevant sections of PCMLTFA, and section 12 of the UNATMO. If there is no need for imminent action, e.g. the issue of a restraint order on an account, consent will usually be given for the MSB provider to operate the account under the provisions of the relevant sections of PCMLTFA, and section 12(2B)(a) of the UNATMO. If a no-consent letter is issued, the MSB provider should act according to the contents of the letter and seek legal advice where necessary.

An MSB provider should ensure SARs filed to the FINTRAC are of high quality taking into account feedback and guidance provided by the FINTRAC in its quarterly report and the CCE from time to time. The purpose of the quarterly report, which is relevant to all financial sectors, is to raise AML/CFT awareness. It consists of two parts, (i) analysis of SARs and (ii) matters of interest and feedback. The report is available at a secure area of the FINTRAC website and Bank of Canada website. MSB provider can apply for a login name and password by completing the registration form available on the FINTRAC website as well as Bank of Canada website or by contacting the FINTRAC directly.

Providing an MLRO acts in good faith in deciding not to file an SAR with the FINTRAC and Bank of Canada, it is unlikely that there will be any criminal liability for failing to report if the MLRO concludes that there is no suspicion after taking

into account all available information. It is however vital for the MLRO to keep proper records of the deliberations and actions taken to demonstrate he has acted in reasonable manner.

However, the statutory defense does not absolve an MSB provider from the legal, reputational or regulatory risks associated with the account's continued operation. An MSB provider should also be aware that a "consent" response from the FINTRAC to a pre-transaction report should not be construed as a "clean bill of health" for the continued operation of the account or an indication that the account does not pose a risk to the MSB provider.

The report must not be discussed with the customer, in accordance with the tipping off provisions of the AMLO. We must not proceed with a transaction to which we await consent from the FINTRAC.

There must be no record on the customer file or on the computer system which refers in any way to suspicious circumstances reporting, money laundering, etc. to avoid the risk of tipping off under the AMLO. It is a criminal offence to inform a customer that a SAR has been submitted or to inform them of an investigation into their affairs. All records of SARs will be kept in the central reporting file, which is kept in the nominated officer's office.

We should conduct an appropriate review of a business relationship upon the filing of an SAR to the FINTRAC, irrespective of any subsequent feedback provided by the FINTRAC, and apply appropriate risk mitigating measures. Filing a report with the FINTRAC and continuing to operate the relationship without any further consideration of the risks and the imposition of appropriate controls to mitigate the risks identified is not acceptable. If necessary, the issue should be escalated to the MSB Provider senior management to determine how to handle the relationship concerned to mitigate any potential legal or reputational risks posed by the relationship in line with Company's business objectives, and its capacity to mitigate the risks identified.

Reporting of a suspicion in respect of a transaction or event does not remove the need to report further suspicious Activities/transactions or events in respect of the same customer. Further suspicious Activities or transactions, whether of the same nature or different to the previous suspicion, must continue to be reported to the MLRO who should make further reports to the FINTRAC if appropriate.

8.5 TIPPING OFF

Any staff member needs to make a judgment as to whether any delay to the transaction ('Consent request') would have the effect of 'tipping off' the customer.

Tipping Off is another offence under the DTROP, the OSCO and the UNATMO. A person commits an offence if, knowing or suspecting that a disclosure has been made, he discloses to any other person any matter which is likely to prejudice any investigation which might be conducted following that first-mentioned disclosure. The maximum penalty for the offence upon conviction is imprisonment for 3 years and a fine.

You should never disclose to the customer"

- that a transaction was/is being delayed because consent from FINTRAC has been requested;
- that details of their transactions or activities will be/have been reported to the FINTRAC and/or to the Bank of Canada;
- that they are being investigated by law enforcement.

9.1 AML/CTF TRAINING OF STAFF/AGENT

Training is given to all staff members and compliance delegate at agent location upon commencement of taking on the money transfer service and on regular occasions afterwards (at least once a year). Training covers the following issues:

- The law relating to financial crime
- Risks associated with the financial crime threat to the company
- Identity and responsibilities of the MLRO
- Internal policies and procedures put in place
- Customer Due Diligence/Enhanced due diligence monitoring measures
- Suspicious activity – what to look out for
- How to submit an internal Suspicious Activity Report to the MLRO
- Record-keeping requirement

The MLRO will take appropriate measures to keep a log of all training which is provided to staff members – a sample of the training log is attached in the appendix.

All staff will be required to sign the training log where required to confirm that they have received training.

The MLRO will circulate to all staff other material to heighten awareness of anti-financial crime issues. This must be placed on the company notice board which should be available in all branch/agent locations.

Where possible, MLRO will arrange for external trainings for the staff and a record will be kept of the training material and results.

All agents must take AML/CFT training before they are permitted to create customer transactions. All agents must receive refresher training annually or on need basis.

10.1 RETENTION OF RECORDS

General Legal Requirements

We will only be successful in demonstrating our compliance with the requirements of the regulations through keeping evidence and records of:

- Due diligence checks made and
- Information held on customers and transactions.

These records are crucial in any subsequent investigation by FINTRAC, the police or other Supervisory Authority in other host state. They will enable the business to produce a sound defense against any suspicion of involvement in money laundering or terrorist financing, or charges of failure to comply with the Regulations.

The records that must be kept are:

- A copy of, or the references to, the evidence of the customer's identity obtained under the customer due diligence requirements in the Regulations. Clear copies of the forms of identification presented by customers, or a record of where they can be obtained, should be retained.
- The supporting evidence and records in respect of the business relationships and occasional transactions which are the subject of customer due diligence measures or on-going monitoring. Records must be kept and should include the name and address of the customer.

In relation to the evidence of a customer's due diligence of the Company and its Agents must keep the following records:

- All copies of documents accepted and verified as evidence for conduct of due diligence and
- all other References to the evidence of customer's identity
- Transaction and business relationship records including evidence of the customers' source of fund (including account files, relevant business correspondence, daily logbooks, receipts, cheques etc.) should be maintained in a form from which a satisfactory audit trail may be compiled, and which may establish a financial profile of any suspect account or customer.

How long the customer due diligence records must be kept?

Evidence of customer's identity records must be kept for minimum of Seven years beginning from the end of the year during which the date of completion of the transaction or the termination of the business relationship occurred.

The same retention period applies to records of transactions (whether undertaken as occasional transactions or part of a business relationship).

In what format must the records be kept?

Records may therefore be kept:

- By way of original documents

- By way of good photocopies of original documents
- In scanned form
- In computerized or electronic form.
-

It must be ensured, however, that the data stored electronically is consistent with the original document.

11.1 INDEPENDENT REVIEW OF Pay4B Limited ANTI-MONEY LAUNDERING PROGRAM

At least once in every two years, the Company will appoint an internal or external reviewer to conduct independent review of its AML program, first review will be carried by the end of 2024. The review will cover the testing of the following area:

- Documented AML and Sanctions Screening Policies and Procedures
- Enterprise-Wide AML Risk Assessments
- Senior Management/Board Approval of AML Program
- How the business ensures that it holds the appropriate authorizations and abides by local laws both where it has an on the ground presence and where it conducts business on a reach-in basis?
- Customer KYC/CDD and EDD Onboarding and Refresh Processes – Test Customer Files. If company adopts Machine Learning KYC ID&V, test escalation process for clients who do not pass ID&V.
- Customer Risk Scoring – Review of Methodology and Risk Matrices
- Transaction Monitoring System – Review of Methodology
- Transaction Monitoring – Alert Process – Testing of Actions on Alerts
- Transaction Monitoring - Review of QA process relating to discounting of Alerts
- Suspicious Activity monitoring, escalation and reporting (SAR)
- Sanction and PEP Screening and Escalation Process
- Sanctions Screening System – Testing of Fuzzy Logic and List Maintenance
- Ongoing Monitoring Process – (Sanctions and Negative News) Testing
- AML system controls and data integrity
- Third Part Payment Process Policy Review and Testing
- Suspicious Activity Reporting Process - Testing
- AML Training – Program and Oversight Process
- Record keeping/retention

Management and key officers to be interviewed, including:

- Accountable Executives for awareness and responsibilities in the AML control Process
- AML Officer
- Compliance Team Leaders
- Business Leads and Support Unit Heads
- Front office management for AML Procedures and Customer Onboarding
- Operational Heads responsible for AML/Sanctions Screening controls
- IT Head for AML/Sanctions Screening operational system controls (transaction monitoring, customer information)
- Quality and Assurance Teams

Scoping must ensure:

- Coverage of the entire AML/Sanctions Screening Program, while also being
- Risk based to allocate the independent reviewer's time and staff resources to areas of greater risk and heavier testing of internal controls

APPENDIX I – RISK ASSESSMENT & MITIGATION

RISK MATRIX/RISK SCORE of Pay4B Limited risk-assessment and AML policy:

LIKELIHOOD	IMPACT		
High likelihood	Medium - 2	High - 3	Extreme - 4
Medium likelihood	Low - 1	Medium - 2	High - 3
Low likelihood	Low - 1	Low - 1	N/A
	Minor	Moderate	Major

Likelihood: the potential of an ML/TF risk occurring in your business for the particular risk being assessed.

Impact (consequence): the seriousness of the loss or damage which could occur should the event (risk) happen

High Likelihood:	Almost certain that risk event will occur several times a year
Medium Likelihood:	High probability that risk event will occur once a year
Low Likelihood:	Unlikely, if not impossible

Major Impact:	Huge consequences – major damage or effect. Serious terrorist act or large scale money laundering
Moderate Impact:	Moderate level of money laundering or terrorism financing
Minor Impact:	Minor or negligible consequences or effects

The risk that Pay4B Limited services will be used for ML/TF. Risk group – Customers

Customer Risk

Customer Risk Factors	Risk Indicator	Likelihood	Impact	Risk Score	Pay 4B Limited Action/ Control(refer Control Library)	Hard wire control which effectively mitigates risk
New customer carrying out large (money remiitance in SEPA / SWIFT) transaction	Transactions are almost always paid in by money remiitance in SEPA / SWIFT to agent	Medium / High	Moderate	Medium 2	• Money remiitance in SEPA / SWIFT transactions maximum threshold • Enhanced Customer Due Diligence • Systems controls (transaction screens) • Monitoring • AML/Compliance awareness training • Assurance processes • Prohibited customers and transactions	1. An absolute ceiling of CAD equivalent of USD 5,000 prevents any transaction above this amount from being processed. Reduced limits apply to particular countries; 2. Multiple transactions by common sender or to common beneficiary to circumvent max threshold limits are tracked by phone number and ID details. System will automatically block second and following transactions – as well as first transaction if payout is still pending.
Non-resident Customer	Possibility for remittance transactions sent overseas by non-residents.	Low	Minor/ Moderate	Low 1	• Customer acceptance • Systems controls (transaction screens) • Enhanced customer due diligence • AML/Compliance awareness training	
Entities that are opaque, personal asset	Transactions by legal, non-individual entities.	Low	Minor	Low 1	• Customer acceptance • Systems controls (transaction screens)	Only individual to individual transactions are permitted - Pay4B Limited system

holding vehicles (e.g. trust, company)					• Enhanced customer due diligence	requires completion of fields including: name/surname, DOB, ID information. No transaction is permitted by a non-individual.
PEP (Politically Exposed Person)	Person whose stated occupation or ID document details or screening results indicate likelihood of PEP status.	Low	Minor	Low 1	• Sanction List screening • Monitoring • Customer acceptance • Systems controls (transaction screens) • AML/Compliance awareness training	
Customer or group of customers making numerous Transactions to same individual/ group	Multiple transactions just below threshold; Multiple transactions to common beneficiary; Multiple transactions from common sender.	Medium	Moderate	Medium 2	• Money remiitance in SEPA / SWIFT transactions Threshold of Zero • Monitoring • Customer acceptance • Enhanced customer due diligence • Systems controls (transaction screens) • AML/Compliance awareness training • Unusual Transaction reporting • Suspicious Activity Reporting	1. An absolute ceiling of CAD equivalent of USD 5,000 prevents any transaction above this amount from being processed. Reduced limits apply to particular countries; 2. Multiple transactions by common sender or to common beneficiary to circumvent max threshold limits are tracked by phone number and ID details. System will automatically block second and following transactions – as well as first transaction if payout is still pending.
Customer who has a business/ occupation which is money remiitance	Customer performs large volume of transactions which are inconsistent with	Low/Medium	Minor/ Moderate	Low 1	• Money remiitance in SEPA / SWIFT transactions maximum threshold • Customer acceptance • Systems controls (transaction	An absolute ceiling of CAD equivalent of USD 5,000 prevents any transaction above this amount from being processed. Reduced limits apply to particular countries.

in SEPA / SWIFT - intensive	customer's profile as individual and stated source of income.				screens) • Enhanced customer due diligence • AML/Compliance awareness training • Monitoring	
Customer who presents unusual or invalid ID	Customers do not always possess common acceptable ID types such as: EU National ID passport or Age proof card.	Low	Moderate/ Major	Medium 2	• Customer acceptance • Enhanced customer due diligence • Monitoring • Assurance processes • AML/Compliance awareness training	Foreign driver licenses and non-photographic ID documents are not acceptable for customer ID verification or transaction identity verification purposes.
Customer ID verifications not done properly	Incomplete or inaccurate customer data provided by customer and accepted by agent; The Company has lower level of control over customer due diligence verification as this is performed by agents*)	Low	Moderate/ Major	Medium 2	• Systems controls (transaction screens) • Enhanced customer due diligence • Monitoring • AML/Compliance awareness training • Assurance processes	Agent must provide confirmation/declaration for each and every transaction that customer verification processes have been performed correctly.
Affiliate agents are typically small businesses (<5 persons); Agents operate in a different industry environment with different business priorities. The knowledge and experience of KYC compliance procedures is of a lesser standard resulting in a lower-level understanding of AML/CTF obligations including significance and ramifications of ML offences – and what constitutes particular ML offences. Remittance services often represent a low proportion of the affiliate agent's business revenue. Therefore, there is a higher risk for inadequate verification processes occurring.						

Product Risk

Product Risk Factors	Risk Indicator	Likelihood	Impact	Risk Score	Pay4B Limited Action/ Control(refer	Hard wire control which effectively mitigates risk

					Control Library)	
Door Delivery Service		Low	Moderate	Low 1	• Customer acceptance • Enhanced customer due diligence • Assurance processes	N/A
Account Credit		Low/Medium	Minor/ Moderate	Medium 2	• Customer acceptance • Enhanced customer due diligence • Assurance processes • Monitoring	
E-services: money remiitance in SEPA / SWIFT to card		Low	Minor	Low 1	• Customer acceptance • Enhanced customer due diligence • Assurance processes • Monitoring	N/A
E-services: money remiitance in SEPA / SWIFT to mobile		Low	Minor	Low 1	• Customer acceptance • Enhanced customer due diligence • Assurance processes • Monitoring	N/A
Money remiitance in SEPA / SWIFT to Money remiitance in SEPA / SWIFT		Medium	Moderate	Medium 2	• Money remiitance in SEPA / SWIFT transactions maximum threshold • Monitoring • Customer acceptance • Enhanced customer due diligence • Systems controls (transaction screens) • AML/Compliance awareness training	1. An absolute ceiling of CAD equivalent of USD 5,000 prevents any transaction above this amount from being processed. Reduced limits apply to particular countries; 2. Multiple transactions by common sender or to common beneficiary to circumvent max threshold

					• Assurance processes • List screening • Suspicious Activity Reporting	limits are tracked by phone number and ID details. System will automatically block second and following transactions – as well as first transaction if payout is still pending.
Face to face transactions – paid out via bank partners (money remiitance in SEPA / SWIFT to money remiitance in SEPA / SWIFT; account credit; money remiitance in SEPA / SWIFT to card; money remiitance in SEPA / SWIFT to mobile)		Low/Medium	Minor/Moderate	Medium 2	• Customer acceptance • Enhanced customer due diligence • Assurance processes • Monitoring • List screening	
Face to face transactions – paid out via direct agent partners (Money remiitance in SEPA / SWIFT to money remiitance in SEPA / SWIFT ; cheque payment; door delivery)		Medium	Moderate	Medium 2	• Customer acceptance • Enhanced customer due diligence • Assurance processes • Monitoring • List screening	
Online/internet (currently not available)		Zero	N/A	N/A 0	No action required	
Likelihood: the potential of an ML/TF risk occurring in your business for the particular risk being assessed. Impact (consequence): the seriousness of the loss or damage which could occur should the event (risk) happen Explanatory						

notes:

'FATF has recognized that specific products, services, transactions or delivery channels may pose a greater risk of money laundering. Examples include private banking, anonymous transactions (which may include money remiitance in SEPA / SWIFT), non-face-to-face business relationships or transactions, and payment received from unknown or un-associated third parties.'

Geographic Risk

Country Risk Factors	Risk Indicator	Likelihood	Impact	Risk Score	Pay4B Limited Action/ Control(refer Control Library)	Hard wire control which effectively mitigates risk
Countries identified by credible sources as not having adequate AML/ CTF systems1	Transactions to countries identified as having deficient AML/CTF systems according to Pay4B Limited country risk indicators. Transactions with any country ranked 7.0 or above on Basel AML Index Country Risk Rating presents this risk.	Medium	Moderate	Medium 2	• Country ML/TF risk index • Monitoring • Red flags • Enhanced customer due diligence • List screening • Suspicious Matter Reporting	1. An absolute ceiling of CAD equivalent of USD 5,000 prevents any transaction above this amount from being processed. Note: Reduced limits apply to particular countries 2. For country corridors where this risk is categorized as High-Extreme, Pay4B Limited makes a determination to exit operations/ distribution network from that country (e.g. Iran, North Korea, Cuba, Somalia etc.).
Countries which are subject to EU trade sanctions1	Country is listed as being subject to sanctions by EU/UN/FATF	Low	Moderate	Low 1	• Country ML/TF risk index • Monitoring • Red flags • Enhanced customer due diligence	Most countries which have UN sanctions in place are categorized as High to Extreme risk, Pay4B Limited consequently does

					• List screening • Suspicious Matter Reporting	not have business in place.
Countries – or geographic areas identified by credible sources as being known to be a significant source of criminal activity*2	Transactions to countries identified as being known to be source of criminal activity according to Pay4B Limited country risk indicators.	Medium	Moderate	Medium 2	• Country ML/TF risk index • Customer acceptance • Enhanced customer due diligence • Agent due diligence processes • Systems controls (transaction screens) • Monitoring from that country • Red flags • List screening • Suspicious Matter Reporting	For country corridors where this risk is categorised as High- Extreme, Pay4B Limited makes a determination to exit operations/ distribution network
Countries – or geographic areas identified by credible sources as being linked to terrorism activity*3	Transactions to countries identified as being known to be source of terrorism activity according to Pay4B Limited country risk indicators.	Low	Major	Medium 2	• Country ML/TF risk index • Monitoring • Red flags • Enhanced customer due diligence • List screening • Suspicious Matter Reporting	1. All countries on US State Dept blacklist (Cuba, Iran, Sudan and Syria) are excluded from Pay4B Limited country network;

Explanatory notes:
*Criminal activity to include: tax haven activity; source of narcotics; corruption; people smuggling; or other significant criminal activity.
**Terrorism activity to include: funding or support provided for terrorist activities or designated terrorist organizations operating within the country.

Regulatory Risk Factors	Risk Indicator	Likelihood	Impact	Risk Score	Pay4B Limited Action/ Control(refer	Hard wire control which effectively mitigates risk

					Control Library)	
Agent conducting transactions while not registered with location jurisdictional regulatory body as the Company's affiliate		Low	Moderate	Low 1	• Agent due diligence processes • Robust Agent f & p assessment • Separation of duties – Employees	Agents are only activated in the Company's system by the Company's Operations Specialists to be able to conduct transactions, once confirmation has been received by the Company's. Compliance department.
Key Personnel not adequately confirmed	Agents with opaque business structure such as company or trust;	Medium	Moderate	Medium 2	Agent due diligence processes Agent ID Verification and Authentication Certified copies of ID documents Operational support by the Company Robust Agent f & p	Applications for registration are not approved by the Company's compliance without full documentation and approval.
Customer ID verifications not done properly	Incomplete or inaccurate customer data entered into the Company's transaction system creating data quality errors for reporting purposes	Low/Medium	Moderate	Medium 2	• Systems controls (transaction screens) • Enhanced customer due diligence • Monitoring • AML/Compliance awareness training • Assurance processes	Agent must provide confirmation/declaration for each and every transaction that customer verification processes have been performed correctly.
Failure to train the Company's staff adequately	Inadequate training records	Medium	Moderate	Medium 2	• AML/Compliance awareness training • Record-keeping • Operational support by the Company	Quarterly Board Meeting Review program for oversight
Not having an AML/CTF	No program in place.	Low	Moderate	Low 1	• AML/CTF Program	Quarterly Board Meeting Review program for

Program						oversight
Failure to generate reports for monitoring and providing support to Agents for regulatory reporting within required time		Low	Minor/ Moderate	Low 1	• Scheduled reports for various parameters (e.g. monthly / half yearly Analysis report) • Employee roles –Pay4B Limited	IT generated reports are scheduled on a monthly basis. Reports generated are cross-checked with an alternative system query to identify transactions that are not captured in IT generation process.
The Company's failure to report suspicious matters		Low/Medium	Moderate	Medium 2	• Monitoring • List screening • Suspicious Matter Reporting • Contract with Affiliate Agents	Quarterly Board Meeting Review program for oversight
Not having an AML/CTF Compliance Report		Low	Moderate	Low 1	• Compliance reporting • Employee roles – Pay4B Limited	Quarterly Board Meeting Review program for oversight
Not having an AML/CTF Compliance Officer		Low	Moderate/ Major	Medium 2	• AML/CTF Compliance Officer role • Employee roles • Board oversight	Quarterly Board Meeting Review program for oversight

Explanatory notes:

- 'A jurisdiction compliant with the FATF Recommendations poses a far lower risk of money laundering generally – including corruption-related money laundering – than a jurisdiction that does not'
- Countries which are determined to represent an unacceptable risk to Pay4B Limited are withdrawn from distribution network (e.g. Iran, Somalia, Afghanistan, Sudan)

Regulatory Risk Factors	Risk Indicator	Likelihood	Impact	Risk Score	Pay4B Limited Action/ Control(refer Control Library)	Hard wire control which effectively mitigates risk
Agent conducting transactions while not registered with local regulatory body as the Company's		Low	Moderate	Low 1	• Agent due diligence processes • Reporting Entity Roll • Agent f&P Assessment Separation of duties -	Agents are only activated in the Company system by the Company Operations Specialists to be able to conduct transactions, once confirmation has been received by the

affiliate					Employees	Company Compliance department.
Agent personnel who meet the criteria of Key Personnel are not declared to the Company	Documentation and observation of agent indicates additional key personnel may be in existence.	Medium	Moderate	Medium 2	• Agent due diligence processes • Agent ID Verification and Authentication • Certified copies of ID documents • Operational support by the Company • Agent f&P Assessment	Applications for registration is verified and/or not submitted to local regulator where the Company is a registered entity without full documentation and declarations received by the Company's Compliance department.
Agent verification not done properly (and subsequent data quality errors in regulatory reporting)	Incomplete or inaccurate customer data provided by customer and accepted by agent leading to data quality errors in regulatory reporting by the Company in applicable jurisdictions.	Low/Medium	Moderate	Medium 2	• Systems controls (transaction screens) • Enhanced customer due diligence • Monitoring • AML/Compliance awareness training • Assurance processes	Agent must provide confirmation/declaration for each and every transaction that customer verification processes have been performed correctly.
Failure by affiliate agent to train staff adequately	Inadequate training records; Systemic errors in customer acceptance and transactions.	Medium	Moderate	Medium 2	•AML/Compliance awareness training • Record-keeping • Operational support by the Company	Regular on-site and off site compliance checks by Compliance Team
Not having an AML/CTF Program	No program in place.	Low	Moderate	Low 1	• AML/CTF program • Assurance processes	• Company on-boarding procedure
Failure to report unusual matters to the Company which may constitute a suspicious		Low/Medium	Moderate	Medium 2	• Unusual matter reporting • Monitoring • List screening • Contract with Affiliate Agents	Regular on-site and off site compliance checks by Compliance Team

matter						
Not having an AML/CTF Compliance Report		Low	Moderate		• Compliance reporting • Employee roles	Regular on-site and off site compliance checks by Compliance Team

APPENDIX II – SAR SUBMISSION FORM

SAR Submission Form

SAR No: _____

Agent Name & Prefix: _____

To: Money Laundering Reporting Officer

From: _____Job Title: _____

I consider the following transaction suspicious and report to you under the internal reporting procedure:

SAR Submission Date: _____/_____ /_____

This SAR is:

- ☐ A request for consent for a transaction which has not yet completed
- ☐ A report on a transaction which has taken place which I consider suspicious
- ☐ Report on other business related activities which I consider suspicious

Transaction Details:			
Sender Name:		Receiver Name:	
Transaction Pin:		Transaction Amount	
Transaction Date:		Transaction Hold Date:	
Reason of Suspiciousness: **Action Taken:** Signed: (Please attach ids and supportive documents)			

Remarks by MLRO: _____

Dated: _____ Signed: _____

NOTE* Following submission of this SAR, the submitter should not discuss the matter with anyone. The MLRO will directly respond with further instructions.

Pay4B Limited

APPENDIX III – SOURCE OF FUNDS DECELERATION FORM

COMPLIANCE FORM – ORIGIN AND PURPOSE OF FUNDS

Date (dd/mm/aa)_____No of transaction_____Transaction No._____ Current Amount_____Total Amount:_____

IDENTIFICACION
Remittent information:

Name(First Name + Last Name) _____
Address_____
TEL_____
City_____Country_____Resident _____
ID document - resident card, passport etc._____
ID Number_____Expiry date_____
Date of birth_____

Job activity_____Country of job activity_____
Place of working_____Job position_____
Employer's TEL._____Employer's address_____
Relationship with beneficiary_____

Origin and purpose of the transfer:

Origin of funds (*)_____
Purpose of the transfer, funds will be used for_____

Beneficiary information:

First Name + Last Name_____Date of birth_____
Address_____TEL_____
City_____Country_____Resident _____No_____
Job activity_____

Sender's undertaking:

I hereby declare that i am not involved in any criminal or money laundering activity and the funds for the above transaction were obtained by me are clear and are not derived from any illegal activities. These funds are derived from the following source.

Agent undertaking:

I/we have examined the photo id/documents of the sender listed above and certify that the sender information recorded matches the information in the ID presented to me/us.

Signature of sender_____

Signature of Agent _____

APPENDIX IV – AML/CTF TRAINING ACKNOWLEDGMENT

Date:
Type: Initial/Refresher

Ref: RPLNo.
Training Conducted by: _____

AML/CTF - TRAINING ACKNOWLEDGMENT

Dear Sir,

I acknowledge the receipt of a copy of Pay4B Limited "Compliance Manual" and confirm that I have read, understood and will comply with the procedures outlined in this manual. I have also undergone the basic AML-training provided by Pay4B Limited. I will likewise give similar training to any of my employees who will conduct transactions on my behalf, or otherwise contact Pay4B Limited to have them trained, before they operate the Pay4B Limited transaction system. I agree to refer any compliance-related questions or difficulties to yourself or to whomever you nominate to act in your absence.

I confirm that compliance at all times with the procedures set out in the manual is a term of our contract with Pay4B Limited. Any breaches to these terms may result in termination of the Pay4B Limited Agreement.

Name: _____

Signature: _____

Date:

APPENDIX V – LAWS AND REGULATIONS

Legislation concerned with ML, TF, financing of proliferation of weapons of mass destruction (PF) and financial sanctions

Role of the Financial Action Task Force (the FATF)

The Financial Action Task Force (the FATF) is an inter-governmental body formed in 1989. The objectives of the FATF are to set standards and promote effective implementation of legal, regulatory and operational measures for combating of ML, TF, PF, and other related threats to the integrity of the international financial system.

The FATF has developed a series of Recommendations that are recognized as the international standard for combating of ML, TF and PF. They form the basis for a co-ordinated response to these threats to the integrity of the financial system and help ensure a level playing field. In order to ensure full and effective implementation of its standards at the global level, the FATF monitors compliance by conducting evaluations on jurisdictions and undertakes stringent follow- up after the evaluations, including identifying high-risk and other monitored jurisdictions which could be subject to enhanced scrutiny by the FATF or counter-measures by the FATF members and the international community at large.

Many major economies have joined the FATF which has developed into a global network for international cooperation that facilitates exchanges between member jurisdictions. As a member of the FATF, **Canada is obliged to implement the latest FATF Recommendations and it is important that Canada complies with the international AML/CFT standards in order to maintain its status as an international financial center.**

Main legislation pieces regulating AML and CFT

The main pieces of legislation in Canada that are concerned with ML, TF, PF and financial sanctions are:

- the AMLO,
- the Drug Trafficking (Recovery of Proceeds) Ordinance, Cap. 405 (DTROP),
- the Organized and Serious Crimes Ordinance, Cap. 455 (OSCO),
- the United Nations (Anti-Terrorism Measures) Ordinance, Cap. 575 (UNATMO),
- the United Nations Sanctions Ordinance, Cap. 537 (UNSO), and
- the Weapons of Mass Destruction (Control of Provision of Services) Ordinance, Cap. 526 (WMD(CPS)O).

It is very important that MSOs and their officers and staff fully understand their respective responsibilities under the different legislation.

Anti-Money Laundering and Counter-Terrorist Financing Ordinance, Cap. 615 (AMLO):

The AMLO imposes requirements relating to customer due diligence (CDD) and record-keeping on MSB Provider and provides the FINTRAC with the powers to supervise compliance with these requirements and other requirements under the AMLO.

In addition, MSB Provider to take all reasonable measures (a) to ensure that proper safeguards exist to prevent a contravention of any requirement under RBA and AML and CTF Systems; and (b) to mitigate ML/TF risks.

The AMLO makes it a criminal offence if an MSB provider (1) knowingly; or (2) with the intent to defraud the FINTRAC regulator of Canada, contravenes a specified provision of the AMLO.

The "specified provisions" are listed in Section 5(11) of the AMLO which are related to CDD requirements and Record-Keeping. If the MSB provider knowingly contravenes a specified provision, it is liable to a maximum term of imprisonment of 2 years and a fine of $1 million upon conviction. **If the MSB provider contravenes a specified provision with the intent to defraud the CCE, it is liable to a maximum term of imprisonment of 7 years and a fine of $1 million CAD upon conviction.**

The AMLO also makes it a criminal offence if a person who is an employee of an MSB provider or is employed to work for an MSB provider or is concerned in the management of an MSB provider: (1) knowingly; or (2) with the intent to defraud the MSB provider or the FINTRAC, causes or permits the MSB provider to contravene a specified provision in the AMLO. **If the person who is an employee of an MSB provider or is employed to work for an MSB provider or is concerned in the management of an MSB provider knowingly contravenes a specified provision, he is liable to a maximum term of imprisonment of 2 years and a fine of $1 million CAD upon conviction. If that person does so with the intent to defraud the MSB provider or the FINTRAC he is liable to a maximum term of imprisonment of 7 years and a fine of $1 million CAD upon conviction.**

The FINTRAC – regulator of Canada may take disciplinary actions against MSB provider for any contravention of a specified provision in the AMLO. The disciplinary actions that can be taken include publicly reprimanding the MSB provider; ordering the MSB provider to take any action for the purpose of remedying the contravention; and ordering the MSO to pay a pecuniary penalty not exceeding the greater of $10 million CAD or 3 times the amount of profit gained, or costs avoided, by the MSB provider as a result of the contravention.

Drug Trafficking (Recovery of Proceeds) Ordinance, Cap. 405 (DTROP):

The DTROP contains provisions for the investigation of assets that are suspected to be derived from drug trafficking activities, the freezing of assets on arrest and the confiscation of the proceeds from drug trafficking activities upon conviction.

Organized and Serious Crimes Ordinance, Cap. 455 (OSCO):

The OSCO, among other things:

a) gives officers of the Canda Police and Prosecution Authorities and the FINTRAC powers to investigate organized crime and triad activities;
b) gives the Courts jurisdiction to confiscate the proceeds of organized and serious crimes, to issue restraint orders and charging orders in relation to the property of a defendant of an offence specified in the OSCO;
c) creates an offence of money laundering in relation to the proceeds of indictable offences; and
d) enables the Courts, under appropriate circumstances, to receive information about an offender and an offence in order to determine whether the imposition of a greater sentence is appropriate where the offence amounts to an organized crime/triad related offence or other serious offences.

United Nations (Anti-Terrorism Measures) Ordinance, Cap. 575 (UNATMO):

The UNATMO is principally directed towards implementing decisions contained in relevant United Nations Security Council Resolutions (UNSCRs) aimed at preventing the financing of terrorist acts and combating the threats posed by foreign terrorist fighters. Besides the mandatory elements of the relevant UNSCRs, the UNATMO also implements the more pressing elements of the FATF Recommendations specifically related to TF.

Under the CCC (Criminal Code of Canada), PCMLTFA, a person commits an offence if he deals with any property knowing or having reasonable grounds to believe it to represent any person's proceeds of drug trafficking or of an indictable offence respectively. The highest penalty for the offence upon conviction is imprisonment for 14 years and a fine of $5 million CAD.

The UNATMO, among other things, criminalizes the provision or collection of property and making any property or financial (or related) services available to terrorists or terrorist associates. The highest penalty for the offence upon conviction is imprisonment for 14 years and a fine. The UNATMO also permits terrorist property to be frozen and subsequently forfeited.

The CCC (Criminal Code of Canada), PCMLTFA and the UNATMO also make it an offence if a person fails to disclose, as soon as it is reasonable for him to do so, his knowledge or suspicion of any property that directly or indirectly, represents a person's proceeds of, was used in connection with, or is intended to be used in connection with, drug trafficking, an indictable offence or is terrorist property respectively. This offence carries a maximum term of imprisonment of 3 months and a fine of $50,000 CAD upon conviction.

"Tipping off" is another offence under the CCC (Criminal Code of Canada), PCMLTFA and the UNATMO. A person commits an offence if, knowing or suspecting that a disclosure has been made, he discloses to any other person any matter which is likely to prejudice any investigation which might be conducted following that first-mentioned disclosure. The maximum penalty for the offence upon conviction is imprisonment for 3 years and a fine.

United Nations Sanctions Ordinance, Cap. 537 (UNSO):

The UNSO provides for the imposition of sanctions against persons and against places outside the People's Republic of China arising from Chapter 7 of the Charter of the United Nations. Most UNSCRs are implemented in Canada under the UNSO.

Weapons of Mass Destruction (Control of Provision of Services) Ordinance, Cap. 526 (WMD(CPS)O):

The WMD(CPS)O controls the provision of services that will or may assist the development, production, acquisition or stockpiling of weapons capable of causing mass destruction or that will or may assist the means of delivery of such weapons. Section 4 of WMD(CPS)O prohibits a person from providing any services where he believes or suspects, on reasonable grounds, that those services may be connected to PF. The provision of services is widely defined and includes the lending of money or other provision of financial assistance.

Financial Sanctions & Proliferation Financing:

The UNSO empowers the Chief Executive to make regulations to implement sanctions decided by the UNSC, including targeted financial sanctions44 against individuals and entities designated by the UNSC or its Committees. Designated persons and entities are specified by notice published in the Gazette or on the website of the Commerce and Economic Development Bureau. It is an offence to make available, directly or indirectly, any funds, or other financial assets, or economic resources, to, or for the benefit of, a designated person or entity, as well as those acting on their behalf, at their direction, or owned or controlled by them; or to deal with any funds, other financial assets or economic resources

belonging to, or owned or controlled by, such persons and entities, except under the authority of a license, granted by the Chief Executive.

The Chief Executive may grant license for making available or dealing with any funds, or other financial assets, and economic resources to or belonging to a designated person or entity under specified circumstances in accordance with the provisions of the relevant regulation made under the UNSO. An MSB provider, seeking such a license should write to the FINTRAC and Bank of Canada.

To combat PF, the UNSC adopts a two-tiered approach through resolutions made under Chapter VII of the UN Charter imposing mandatory obligations on UN member states:

a) global approach under UNSCR 1540 (2004) and its successor resolutions; and
b) country-specific approach under UNSCR 1718 (2006) against the Democratic People's Republic of Korea (DPRK) and
c) UNSCR 2231 (2015) against the Islamic Republic of Iran (Iran) and their successor resolutions.

The counter proliferation financing regime in Canada is implemented through legislation, including the regulations made under the UNSO which are specific to DPRK and Iran, and the WMD(CPS)O. Section 4 of WMD(CPS)O prohibits a person from providing any services where he believes or suspects, on reasonable grounds, that those services may be connected to PF. The provision of services is widely defined and includes the lending of money or other provision of financial assistance.

Sanctions imposed by other Jurisdictions:

While, MSB provider do not normally have any obligation under Canadian laws and regulations to have regard to unilateral sanctions imposed by other organizations or authorities in other jurisdictions, an MSB provider, operating internationally will need to be aware of the scope and focus of relevant sanctions regimes in those jurisdictions. Where these sanctions regimes may affect its operations, the MSB provider should consider what implications exist for its procedures and take appropriate measures, such as including relevant overseas designations in its database for screening purpose, where applicable.

APPENDIX VI – DATA PROTECTION REQUIREMENTS IN RELATION TO AML

Background to the PIPEDA:

Canada is one of Northern America's earliest adopters of comprehensive data privacy regulation. The Personal Information Protection and Electronic Documents Act (hereinafter referred as the PIPEDA), adopted in 2000 and came into effect in stages between 2001 and 2004. Due to recent data privacy incidents, which occurred at 2017 due to Equifax Data Breach (when around 100 000 Canadian residents have been compromised, including their names, addresses and credit card information), Desjardins Data Breach, which occurred at 2019 (this breach of data, involved a former employee, leaked the personal data of over 4.2 million members, including names, addresses and financial information) as well as MediTrust Data Breach, occurred in the early 2021 (this data breach affected medical records of patients, exposing sensitive health information and general data of each patient, including their names, address and date of birth) and all of these events have led to an overhaul of the regulatory regime in 2024 and a subsequent stepping up of enforcement action. Reforms brought into discussions by the government and the regulator have made Canadian regulation of data protection amongst the most stringent in the world.

Canadian Privacy Commissioner for Personal Data (the Commissioner) Mr. Phillippe Dufrense, appointed in 2022 as the Head of Office of the Privacy Commissioner of Canada (OPC) is now very active and regularly publishes official guidance on a wide range of topics. Guidance on PIPEDA Compliance (GPIPEDA Compliance), Data Protection Impact Assessments (DPIAs), Privacy Impact Assessments (PIAs), Privacy Management Programs (PMP) as well as recent Digital Charter Implementation Act (DCIA) and Privacy Act Review (PAR) calls for businesses to adopt comprehensive Privacy Management Programs, directed at achieving compliance in all aspects of business. With increased fines, an activist regulator, a policy of "naming and shaming" those who fail to comply and a growing public interest in data privacy issues, it is clear that PIPEDA compliance has to be a priority for Canadian businesses.

The Commissioner and his Powers:

The Commissioner can investigate complaints of breaches of the PIPEDA, as well as initiate investigations. The approach to enforcement is generally administrative and consultative in nature, but the scope for criminal enforcement has recently been broadened and the penalties for non-compliance have been increased.

At the conclusion of an investigation, the Commissioner can issue an enforcement notice against the "data user" (ie the business controlling the data processing), requiring it to take remedial action.

The Commissioner can institute civil or criminal proceedings against any data user that fails to comply with an enforcement notice, depending on the nature of the breach. Maximum penalties for breaches under the PIPEDA are fines of up to CAD $1m (US $ 742,000) and imprisonment for up to five years.

Quite apart from the criminal sanctions, there are reputational risks for an organization that is subject to an investigation. The Commissioner has the right to publish the results of any investigation, name the organization, involved and give details of the breaches committed.

What is Personal Data?

The PIPEDA draws from the OECD's Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, the guidelines which are the cornerstone for Europe's Data Protection Directive EC95/46.

The PIPEDA defines "personal data" very broadly and includes any data relating directly or indirectly to a living individual from which it is practicable for the identity of the individual to be directly or indirectly ascertained.

Does the PDPO have Extraterritorial Effect?

The PIPEDA does not include any express limitation on its territorial scope. However, some limitation may be implied from the discretion the Commissioner has to refuse to investigate a complaint which does not meet one of the following requirements:

I. The investigation relates to the personal data of Canadian citizens and tax-residents or persons who were in Canada at the relevant time; or
II. The investigation relates to data users that are able to control the collection, holding, processing or use of the relevant personal data from Canada.

On What basis can Personal Data be Processed?

"Processing" in relation to personal data, is defined to include amending, augmenting, deleting or rearranging data, by automated or other means. Subject to specific exemptions, personal data can only be processed for the purposes notified to the data subject on or before the collection of the data and any directly related purpose. Data subjects must consent to any new or additional purpose.

The PIPEDA contains a number of exemptions to these requirements, including an exemption for national security interests and exemptions for matters such as disclosures to law enforcement officials and processing in connection with legal proceedings.

Do Data owners need to Register with or notify any Authorities, or Appoint an Official Compliance Officer?

There is no need to register with or notify any authorities of data processing, nor is there any requirement to appoint an official compliance officer. However, data users must provide data subjects with the name or job title and address of the individual who will be responsible for handling data access requests.

In practical terms, it is becoming increasingly important to have senior internal roles that include responsibility for PDPO compliance. The Commissioner's Guidance on PIPEDA Compliance (GPIPEDA Compliance), Data Protection Impact Assessments (DPIAs), Privacy Impact Assessments (PIAs), Privacy Management Programs (PMP) as well as recent Digital Charter Implementation Act (DCIA) and Privacy Act Review (PAR), dealing with Privacy Management Programs makes clear that significant organizational measures are the expected standard for compliance.

What Rights do Data Subjects have to Access and Correct their Data?

Data subjects have the right to know whether or not a business holds personal data about them. They have the right to access and make corrections to that data. Data users may refuse to comply with a request for access or a correction, but must be prepared to give reasons for doing so within 40 days of receipt of a proper request. They may charge a fee for producing the personal data.

Are there any Restrictions on Transfers of Personal Data to third Parties? Or within a Group of Companies?

Personal data cannot be transferred to another data user without the data subject's consent. Where transfers are made for direct marketing purposes, the special requirements set out in the section below entitled "How is direct marketing regulated?" apply.

The PIPEDA draws no distinction between related and unrelated entities, meaning that transfers within groups of companies are in principle regulated to the same standards. There is no requirement under the PIPEDA to obtain a data subject's consent to transfer personal data to a data processor (i.e., a person or entity which processes personal data on behalf of a data user). As a matter of practice, however, data users often notify data subjects that third party processing will be taking place.

Eight Principles of Data Protection:

a) It must be processed fairly and lawfully. We must inform individuals about how the Company uses their personal data;
b) It must be obtained only for specific lawful purposes;
c) It must be adequate, relevant and not excessive. We must only collect the minimum amount of personal data to support the Company’s business activities;
d) It must be accurate and kept to date;
e) It must be processed in accordance with the rights of data subjects. We must be receptive to queries or requests made by individuals in connection with their personal data and where required by law, we must provide individuals with ability to access, correct and delete their personal data;
f) It must not have held for any longer than necessary;
g) It must be protected in appropriate ways, we need to prevent the misuse or loss of personal data and to prevent unauthorized access;
h) It must not be transferred outside Canada, unless that country or territory also ensures an adequate level of protection, or other laws required us to (e.g. Wire Transfer Regulation 2).