AML POLICY

Rules of procedure and internal audit rules compiled pursuant to Money Laundering and Terrorist Financing Prevention Act

AML Policy – January 2026

1.List of abbreviations

AML law	Proceeds of Crime (Money Laundering) and Terrorist Financing Act (S.C. 2000, c. 17) last amended on 2023-06-22
AML / CFT prevention	Measures in the field of prevention of money laundering and terrorist financing (Anti-Money Laundering / Countering the Financing of Terrorism)
ML/FT	Money Laundering / Financing of Terrorism
EEA	European Economic Area
EU	European Union
FINTRAC	Financial Transactions and Reports Analysis Centre of Canada
STR	Suspicious transaction notification/ suspicious transaction report
PEP	Politically Exposed Person
Sanctions Law	Canadian sanctions legislation
SIP	A system of internal policies, procedures and control measures to fulfill the obligations set out in the AML bylaw
CDD	Customer Due Diligence
PEP	Politically Exposed Person
RBA	Risk-Based Approach
SoF	Source of Funds

SoW	Source of Wealth

AML/ATF	anti-money laundering and anti-terrorist financing
FATF	Financial Action Task Force
FIU	financial intelligence unit
APG	Asia/Pacific Group on Money Laundering
ARIN	Asset Recovery Interagency Network
CBSA	Canada Border Services Agency
CFATF	Caribbean Financial Action Task Force
CIFA-BC	Counter Illicit Finance Alliance of British Columbia
CIFG	Counter ISIL Finance Group
COSUN	Co-operating and Supporting Nation
CRA	Canada Revenue Agency
CSIS	Canadian Security Intelligence Service
FLSC	Federation of Law Societies of Canada

FSRB	FATF-style Regional Body

GAC	Global Affairs Canada
IMLIT	Integrated Money Laundering Investigative Team
ISED	Innovation, Science and Economic Development Canada
NIRA	National Inherent Risk Assessment
OECD	Organisation for Economic Co-operation and Development
OSFI	Office of the Superintendent of Financial Institutions
PPSC	Public Prosecution Service of Canada
PSPC	Public Services and Procurement Canada
RCMP	Royal Canadian Mounted Police
RPAA	Retail Payment Activities Act
TBML	trade-based money laundering
- •	- main paragraph • subparagraph

$	All amounts are in Canadian dollars

2.Definition of terms

Terrorism financing	The collection or provision of funds or other property with the knowledge that it will be used, even in part, to commit a crime of terrorism, terrorist attack or a crime intended to facilitate or facilitate the commission of such a crime, or to support a person or group of persons preparing to commit such an offense; Acting to provide remuneration or compensation to the perpetrator of a crime of terrorism, a terrorist attack or a crime intended to enable or facilitate the commission of such a crime, or a close person within the meaning of criminal law, or to raise funds for such compensation or compensation.
L e g a l i z a t i o n o f proceeds of crime	Acts aimed at concealing the illegal origin of any economic advantage resulting from the crime in order to give the impression that it is a property benefit acquired in accordance with the law; such conduct consists, for example: - in the conversion or transfer of property by knowing that it is acriminal offense, in order to conceal or obscure its origin, or in order to assist a person who also participates in the activity to escape the legal consequences of his or her conduct; - in the acquisition, possession, use or disposal of property, knowing that it is derived from criminal activity, - in a criminal organization or other form of co-operation for thepurpose of the above conduct. It is not decisive whether the above-mentioned conduct took place or is to take place in whole or in part in the territory of the Canada or abroad.

Opaque ownership structure	State when it is not possible to find out who is the real owner ofthe client: - from the extract from the Commercial Register other similar documents on the country of residence of foreign persons, whichis not registered in the Commercial Register in the Canada and is not a country - from another instrument on which the foreign person was basedand which contains all its additions, or - from a credible source on which the liable person reasonablyrelies
Trade	Any conduct of the liable person with another person, if such conduct is aimed at disposing of the property of that other personor at providing a service to that other person
Business relationship	A contractual relationship between the liable person and anotherperson whose purpose is to dispose of the property of that other person or to provide services to that other person, if it is clear atthe time of the contractual relationship, taking into account all the circumstances, that it will contain recurring performance
Suspicious business	A transaction carried out in circumstances which give rise to suspicion of attempting to launder the proceeds of crime or a suspicion that the funds used in the transaction are intended to finance terrorism. Circumstances that arouse suspicion may be, for example, anomalies in the client's behaviour compared to hisusual behaviour or compared to the behaviour of a set of clients of a similar type
Identity card	A document issued by a public administration body stating the name and surname, date of birth and from which the form is evident, or other information enabling the person submitting thedocument to be identified as its authorized holder

Country of origin	- in the case of a natural person, this is any state of which this person is a national and at the same time all other states in whichhe is registered for permanent or other residence, - in the case of a legal person which has branches or majority- owned subsidiaries in non-EU or EEC Member States, this is theState in which it has its registered office, - a legal person who has a branch or a majority owned subsidiaryin the countries mentioned above is the state in which he has his registered office and at the same time all the states in which he has a branch, organisational unit or establishment.

The real owner	- In the case of an entrepreneur, a natural person who, in fact or in law, exercises directly or indirectly a decisive influence over the management or operation of that entrepreneur's business (indirect influence means influence exercised through another person or persons), or a natural person who, alone or in agreement with another partner or partners, has more than 25% of the voting rights of this entrepreneur; the disposal of voting rights means the possibility to exercise voting rights at its own discretion, regardless of whether and on what legal ground they are exercised, or the possibility to influence the exercise of voting rights by another person, or - Natural persons acting in concert who hold more than 25% of the voting rights of that entrepreneur, or a natural person who, on the basis of another fact, is the recipient of income from the activities of this entrepreneur, b) at a foundation or endowment fund. - A natural person who is to receive at least 25% of the funds distributed, or if it has not been decided who will be the recipient of the revenues of the foundation or endowment fund, natural person or group of persons in whose interest they were established or in whose interest they work with an association, institute, public benefit company or other similar person in case of trust or other similar relationship under foreign law, a natural person, which has more than 25% of their voting rights or property, or Which is to receive at least 25% of the funds distributed, or in the interest for which they were established or in the interest which they operate, unless it has been decided who will be the recipient of their proceeds

Risk	Risk is the likelihood of a negative occurrence or event happening and its consequences. In simple terms, risk is a combination of the chance that something may happen and the degree of damage or loss that may result. In the context of ML/TF, risk means: At the RE level: Internal and external threats and vulnerabilities that could open an RE up to the possibility of being used to facilitate ML/TF activities. For example, a possible ML/TF risk at the RE level could be conducting business with clients located in high-risk jurisdictions or locations of concern. Threats: A person, group or object that could cause harm. In the ML/TF context, threats could be criminals, third parties facilitating ML/TF, terrorists or terrorist groups or their funds. Vulnerabilities: Elements of a business or its processes that are susceptible to harm and could be exploited by a threat. In the ML/TF context, vulnerabilities could include weak business controls or high-risk products or services.

3.Introduction

These Rules of procedure and internal audit rules are prepared by MINTPAY LTD., an Canadian private limited company, registered under registry code BC1539803, whose legal address is 300-3665 KINGSWAY, VANCOUVER, BC, V5R 5W2, CANADA.

The Company adopts appropriate, sufficient measures aimed to preventing its operations from being used as means to conceal, manage, invest or use any form of money – or other assets – due to illicit activities, or to give the appearance of legality to such activities.

The company adopts a risk-based approach in the design and implementation of this Program with a view to managing and mitigating ML/TF risks. A qualified AML Officer has been appointed to implement appropriate AML/CTF policies and procedures.

4.Money Services Business (MSB)

- MINTPAY LTD. is an MSB in Canada because it offers one or more of the money services business services and has a place of business in Canada. MSBs are subject to regulations and oversight by the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) to prevent money laundering and terrorist financing. Money services businesses must implement a compliance program that will help to ensure the regulatory requirements are met.
- MINTPAY LTD. (hereinafter referred to as "the Company") falls under the classification of a Money Services Business (MSB) in accordance with Canadian law. The designation as an MSB is attributed to the Company's provision of one or more money services business services within the Canadian jurisdiction, coupled with the establishment of a physical presence, or a "place of business," on Canadian soil. The MSB classification carries with it a range of statutory obligations, regulatory mandates, and stringent oversight measures, all aimed at safeguarding the financial system against the risks of money laundering and terrorist financing activities.
- Being a registered MSB, MINTPAY LTD. operates under the purview of the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC), the primary regulatory authority responsible for the enforcement of anti-money laundering (AML) and counter-terrorist financing (CTF) measures in the country. FINTRAC is mandated to monitor, regulate, and supervise the activities of MSBs, ensuring their compliance with the legal framework and standards designed to mitigate financial crime risks.
- The regulatory framework established for MSBs in Canada necessitates the implementation of a comprehensive compliance program. This program serves as a fundamental tool to guarantee that all statutory requirements and obligations, as prescribed by Canadian law and further elaborated upon by FINTRAC, are consistently met and adhered to. The primary objective of the compliance program is to enhance vigilance against money laundering and terrorist financing within the MSB's operations and transactions.

- This compliance program obliges the Company to take an organized approach to risk management, detection, and reporting of any suspicious financial activities that may indicate money laundering or terrorist financing. Furthermore, it mandates the development of a suite of internal policies, procedures, and controls designed to foster transparency, accountability, and security in the operations of the MSB.
- In the subsequent sections of this Anti-Money Laundering (AML) and Counter-Terrorist Financing (CTF) Policy, we will delve deeper into the specific components, requirements, and methodologies governing the Company's compliance program, ensuring a comprehensive and robust approach to financial security and integrity.

5.Company's Compliance Program

- The Compliance Program is grounded in the relevant AML/CTF laws, regulations, and regulatory guidance provided by Canadian Government Institutions. A Compliance Program, mandated for reporting entities (REs), is established to ensure their adherence to the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA) and its associated Regulations. It serves as the foundation for meeting reporting, record-keeping, client identification, and other know-your-client requirements under the PCMLTFA and its associated Regulations. All REs are obligated to establish and implement such a program.
- The purpose of this Program is to establish fundamental AML and CTF procedures and standards, which the Company will rigorously follow. Additionally, it aligns with the Financial Action Task Force (FATF) Standards concerning the prevention of money laundering and the financing of terrorism and proliferation.
- This Program, among other aspects:

• Constitutes an integral component of the Company's broader compliance framework, tailored to meet the legal obligations of its operating environment.

• Enables the Company to identify suspicious activities related to money laundering, fraud, and terrorist financing, subsequently reporting them to the relevant authorities.

Measures for Risk Management and Incident Response:

To comply with the RPAA requirements, the company implements a comprehensive approach to operational risk management and incident response. Key elements include:

1. Identification and assessment of operational risks:
   - Identifying and analyzing potential risks, including cyberattacks, fraud, data breaches, and system failures.
   - Regularly updating risk assessments based on changes in business operations and regulatory requirements.
2. Documentation of response procedures:
   - Developing a clear incident response plan that includes:
     - Steps for mitigating the impact of incidents.
     - Contact details of responsible personnel.
     - Guidelines for notifying internal and external stakeholders.
3. Testing and updating the recovery plan:
   - Regularly testing the recovery plan to ensure its effectiveness.
   - Updating the plan based on test results and emerging risks.
4. Annual reports to the Bank of Canada:
   - Reports must include a description of risks, incident response plans, and details of measures taken to protect customer funds.

The company is committed to maintaining an up-to-date risk management system and adapting it to changes in the regulatory environment.

6.Review of the Program

- The Program is subject to an annual review by the CEO and the AML Officer. The Company's AML Officer may schedule reviews of this Program more frequently as deemed necessary. The Company is obliged to review and, if required, update this Program and its annexes, including the risk assessment policy and the assessments made therein, in the following circumstances:

- Upon the European Commission's publication of the results of a European Union-wide risk assessment on money laundering and terrorist financing.
- Upon the publication of the results of the National Money Laundering and Terrorist Financing Risk Assessment.
- Upon receiving an order from the FINTRAC to enhance the applicable internal procedures.
- In the event of significant events or changes in the Company's management and operations.
- If the necessity arises during periodic monitoring of the implementation and adequacy of the Company's internal policies.

- The review of this Program, including the regular annual review, shall be formally confirmed through a relevant resolution signed by the CEO and the AML Officer.

7. Business Model Summary

- MINTPAY LTD. offers financial services primarily catering to businesses, which encompass the following key areas:

- Foreign exchange dealing.
- Money transferring.
- Payment service provision.

- MINTPAY LTD. primarily operates using a business-to-business (B2B) model. The company's principal focus is to function as a payment service provider, serving both corporate and individual clients.
- The majority of MINTPAY LTD.'s transaction volume is attributed to payment services and foreign exchange dealing.
- Typically, foreign exchange transactions precede remittance transactions to facilitate currency conversion from the sender's currency to the recipient's currency.
- MINTPAY LTD. offers foreign exchange services through partnerships with liquidity providers, including FX brokers, banks, and other licensed remittance operators in Canada and abroad.
- The company does not accept cash payments from customers at present.
- MINTPAY LTD. does not partake in, support, or associate with Initial Coin Offerings (ICOs) or other cryptocurrencies that may be considered securities.

- The company does not engage with any form of store of value, currency, or other products that may constitute a security. Additionally, MINTPAY LTD. does not endorse, participate in, or affiliate with security tokens.
- Business clients, for the purpose of this policy, are defined as entities that currently maintain a contractual relationship with MINTPAY LTD.

8.Regulatory Overview

MINTPAY LTD. is a Canadian money services business (MSB) operating under registration number C10001569, offering the following services:

- Foreign exchange dealing
- Dealing in virtual currencies (transfers and exchanges)
- Payment Services Provider (PSP) activities
- Issuing or redeeming money orders, traveller's cheques, or similar negotiable instruments, excluding cheques payable to a named person or entity
- Remitting or transmitting funds by any means, including through third parties or electronic funds transfer networks

MINTPAY LTD. does not provide the following services:

- Cheque cashing payable to a named person or entity
- Unlicensed casino or gambling services.
- unlicensed forex companies
- unlicensed cryptocurrency exchanges
- Production or trade in weapons and munitions.
- Production or trade in alcoholic beverages (including beer and wine).
- Production or trade in tobacco.
- Production or trade in pharmaceuticals subject to international phase outs or bans.
- Production or trade in pesticides/herbicides subjected to international phase outs or bans.
- Production or activities involving harmful or exploitative forms of forced labor/ harmful child labor.

• Production, trade, storage, or transport of significant volumes of hazardous chemicals, or commercial scale usage of hazardous chemicals.

- MINTPAY LTD. and its affiliated entities are committed to adhering to the rules and regulations stipulated by Canada's Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA) and aim to adopt best practices for MSBs wherever feasible.
- MINTPAY LTD. is obligated to:

• Report eligible transactions.

• Verify client identities in accordance with MSB guidelines.

• Facilitate independent reviews of our compliance program.

• Facilitate regular employee training in AML/CTF.

• Maintain a risk assessment and employ a risk-based approach to service delivery.

- The Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) exercises regulatory oversight over the MSB industry, and MINTPAY LTD. is duly registered with FINTRAC, as noted above.
- MINTPAY LTD. has established a comprehensive compliance regime that aligns with the requirements for MSBs under the PCMLTFA.
- MINTPAY LTD. may be subject to audits conducted by FINTRAC, the Canadian Securities Commission, or other regulatory entities.
- MINTPAY LTD. fully supports FINTRAC's initiatives to mitigate and combat illicit activities and commits to providing reasonable assistance to FINTRAC and its designated entities in the event of an audit or a reportable event.

9. Travel rule

The travel rule is the requirement to ensure that specific information (listed below) is included with the information sent or received in an EFT or a VC transfer ((PCMLTFA), S.C. 2000, c 17, s. 9.5 and PCMLTFR, SOR/2002-184, ss. 124 and 124.1). MINTPAY LTD. commits to including the following information in virtual currency transfers: sender's name, address, account number (if applicable), financial institution details, and transaction amount. We also commit to taking reasonable measures to obtain any missing information before completing the transaction. Any non-compliance will be logged and reported to FINTRAC within 24

hours. Information received under the travel rule cannot be removed from a transfer. (PCMLTFA, S.C. 2000, c 17, s. 9.5.)

FATF Recommendations

FATF Recommendations, while non-binding, are considered "best practices" for Financial Intelligence Units (FIUs) and the entities they oversee. Of particular importance is Recommendation 16, which directly addresses virtual asset service providers and remittance providers:

- Virtual asset service providers (VASPs) and Payment Service Providers (PSPs) must register with local FIUs.
- FIUs should exercise supervision and regulation over VASPs and PSPs.
- VASPs and PSPs must establish a customer identification program for clients whose usage exceeds a threshold of $1,000.
- VASPs and PSPs should provide Know Your Customer (KYC) and other requested information to law enforcement and relevant third parties.
- VASPs and PSPs must comply with international requests for information from law enforcement and regulatory bodies.

Travel Rule (FINTRAC) / (BSA) Rule [31 CFR 103.33(g)]. (additional §20)

- Commonly known as the "travel rule," this regulation mandates financial institutions to share specific information for any transaction involving one or more financial institutions. The required travel rule information for VC and EFTs is:

- Transmitter name, account number, address, banking/financial institution details, amount of the transaction, date of the transaction.
- The name and address of the beneficiary; and if applicable, the beneficiary's account number or other reference number.
- - Recipient banking/financial institution details, name, account number, address.
- The name, address and the account number for VC or other reference number (if any) of the person or entity who requested the transfer (originator information); and the name, address and the account number or other reference number (if any) of the beneficiary.

As a result, MINTPAY LTD. diligently adheres to "best practices" concerning AML/ CTF regulations whenever feasible in the course of our business operations.

If a virtual currency transfer is received and does not have the required travel information, reasonable measures must be taken to obtain that information.

• The originator information will have already been obtained by the Client, because the Client will have been the originator; and

• The beneficiary information will be the Company, as the Company will not be receiving the cryptocurrencies on behalf of any third party rather only on its own behalf in connection with the purchase by the Company of cryptocurrency from the Client.

The Company takes the following reasonable measures to obtain information on received virtual currency transfers:

The Company runs blockchain analysis to determine whether the sending wallet address has been associated with any other virtual asset service provider (VASP), such as an identified cryptocurrency exchange, in order to ensure that the Client for the respective transaction is the originator.

If the Company's due diligence pertaining to the Travel Rule Information is inconsistent with the information provided by the Client, then the Company will suspend the completion of the applicable transaction until such discrepancy is resolved. The liable person sends a report to FINTRAC within 24 hours after the transaction and follows further instructions of FINTRAC.

10. Primary Legislation Governing AML/CTF in Canada

In adherence to the stringent regulatory framework surrounding Anti-Money Laundering and Counter-Terrorist Financing (AML/CTF) in Canada, the Company is mandated to comply with a multitude of legislative instruments and regulatory provisions. A thorough understanding of these legal foundations is imperative for the Company's operation in the jurisdiction. The following is an intricate elucidation of the primary legislations and regulations which govern AML/CTF compliance in Canada.

Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA): At the nucleus of the Canadian AML/CTF framework lies the Proceeds of Crime

(Money Laundering) and Terrorist Financing Act. This pivotal legislation establishes the overarching legal and operational requirements for combating money laundering and the financing of terrorism within Canada. The Company is unequivocally bound by the provisions set forth in the PCMLTFA.

Financial Transactions and Reports Analysis Centre of Canada (FINTRAC):The Company is subject to the authoritative directives of the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC). As Canada's premier governmental agency responsible for AML/CTF oversight, FINTRAC formulates and enforces compliance standards, mandates, and operational guidelines that the Company must diligently observe.

Canadian Anti-Money Laundering Regulations: To provide granular guidance on how reporting entities, including the Company, must fulfill their AML/CTF obligations, the Canadian Anti-Money Laundering Regulations present specific requirements and standards. These regulations are pivotal in implementing AML/CTF measures effectively.

Office of the Superintendent of Financial Institutions (OSFI) Guidance: As a crucial regulatory authority within the Canadian financial sector, the Office of the Superintendent of Financial Institutions (OSFI) issues guidance that the Company is expected to adhere to meticulously. This guidance further refines the AML/CTF framework to ensure the integrity and soundness of financial institutions.

United Nations Act: Canada's adherence to international sanctions is governed by the United Nations Act. The Company is required to demonstrate strict compliance with these sanctions, thus contributing to Canada's international efforts to counteract unlawful financial activities.

Reporting of Suspicious Transactions Regulations: The Company is bound by regulations that dictate the procedures for reporting suspicious transactions. The Company is required to report suspicious transactions to the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) in accordance with the Reporting of Suspicious Transactions Regulations. These regulations are designed to strengthen Canada's anti-money laundering and counter-terrorist financing efforts. When the Company identifies a transaction that appears suspicious, they must report it to FINTRAC, providing relevant details and information. Compliance with these

reporting requirements is crucial, and failure to do so can result in legal consequences and penalties.

Large Cash Transaction Reporting: Regulations mandating the reporting of cash transactions exceeding specified thresholds are integral to the Company's operations. These regulations ensure that large cash transactions are scrutinized and reported as required by law. In Canada, financial institutions are mandated to report cash transactions exceeding $10,000 CAD or its equivalent in foreign currency as part of their anti-money laundering (AML) and counter-terrorist financing (CTF) obligations. The Company's unwavering commitment to upholding the highest standards of AML/CTF measures is rooted in its firm belief that a reputation for integrity and transparency is paramount to achieving its commercial objectives and fulfilling its corporate responsibilities. It is incumbent upon the Company to not only comply with these diverse and multifaceted legal and regulatory provisions but also to actively align with internationally recognized best practices to prevent the illicit use of its services for money laundering and terrorist financing purposes.

11. Effective Controls

- To ensure proper implementation of AML/CTF procedures and controls, Company has effective controls covering:
  - Effective AML/CTF compliance program
  - Senior management oversight
  - Appointment of the AML Officer and other employees with certain responsibilities
  - Compliance and audit function
  - Staff training.
- The CEO of Company is responsible for managing the business effectively and for the oversight of internal AML/CTF controls and systems. The CEO appoints the AML Officer who has overall responsibility for the establishment and maintenance of Company's AML/CTF systems and is the central reference point for suspicious transaction reporting.

Customer Funds Protection Measures

To comply with the RPAA standards, the company commits to implementing the following measures for safeguarding customer funds:

1. Segregated storage of customer funds:

- All customer funds are held in segregated accounts, separate from the company's operational funds.
- Customer funds may only be used to fulfill obligations toward the customers.

2. Funds movement monitoring:

- Implementing a system to monitor and manage the movement of funds to detect anomalies.
- Conducting regular internal checks to ensure compliance with established procedures.

3. Customer notifications:

- In the event of threats or incidents related to the safety of customer funds, the company promptly notifies the customers and provides details of the actions taken.

12. Accountability and Commitment

MINTPAY LTD. is committed to deterring and combating ML/TF both in our systems and the world at large.

MINTPAY LTD. has adopted a risk-based approach and compliance strategy that is approved by a senior officer.

Per this policy and other related policies, MINTPAY LTD. is committed to full compliance with requirements that are designed to deter and detect actual/potential ML/TF as well as other activities that enable/facilitate, or are related to, ML/TF such as fraud.

MINTPAY LTD. encourages and actively develops an internal culture of compliance and ethics among staff, see other policies for details. MINTPAY LTD.. dedicates resources to compliance and risk management

including implementing the below recommendations from FINTRAC for a sufficient compliance regime:

• Appointment of a dedicated, knowledgeable liable person.

• Development and maintenance of a risk management program.

• Documented training program for all Capi Money Canada Ltd. staff.

• Development and application of internal policies, processes, and other initiatives directly related to AML/CTF.

• Regularly scheduled independent reviews to assess the efficacy and relevance of the regime.

• liable person that an independent review is required every 1 year.

• First independent review is due by 2025-09-05 (i.e. within 1 year from the date of MSB registration).

MINTPAY LTD. must renew our FINTRAC MSB registration every 3 years. If MINTPAY LTD. ceases offering MSB services for any reason, we must notify FINTRAC within 30 days of cessation of service.

MINTPAY LTD. recognizes that part of any effective compliance regime is protection for those who comply or attempt to comply in good faith. MINTPAY LTD. supports the requirement for personnel to identify and report suspicious or otherwise reportable transactions to FINTRAC and will attempt to protect said staff from civil and criminal proceedings where possible.

13. Customer Due diligence measures

Customer due diligence measures shall also be applied in the event of suspicion of money laundering or terrorist financing or if the Company has doubts about the correctness of the documents or other data submitted by a customer, i.e. when circumstances differing from ordinary behavior and referring to the existence of risk factors of impact become evident in a customer's actions. Customer due diligence measures shall also be applied in a situation where it is reasonable to presume that it may constitute money laundering or terrorist financing or where the Company is not convinced of the sufficiency of the applied measures. The list of customer due diligence measures set out in the Money Laundering and Terrorist Financing

Prevention Act contains the minimum criteria and is imperative. The
Company shall also take other customer due diligence measures that have not been provided by law, given the customer's field or region of activity as well as the characteristics of the transaction and related risks.
The Company shall, in addition to the customer due diligence measures provided by law, comprehensively evaluate the substance and purpose of the customer's transactions and actions, relying on the universally recognised professional skills characteristic of credit institutions and financial institutions to identify a possible link between a transaction, step or funds and money laundering or terrorist financing.
The Company has sufficiently applied the customer due diligence measures for the purposes of the PCMLTFA if it is convinced that it has sufficiently applied the obligation arising from the aforementioned provision. The principle of reasonableness is taken into account upon assessing conviction.

14. Client Intake and Authentication

- 1 Client Demographics:

1. MINTPAY LTD.'s primary clientele consists of business entities headquartered in Canada, the UK, Europe.
2. MINTPAY LTD. provides services to clients through online and non-face-to- face channels.

- 2 Universal Intake Procedure:

1. The Customer Intake Procedure applies universally to all clients, irrespective of the application method, and is aligned with FINTRAC guidelines for the identification of organizations.
2. Additional due diligence measures may be applied as deemed necessary based on the risk level.

- 3 Organization Verification:

• 3.1 Verification of organizations is accomplished by cross-referencing with pertinent state, provincial, or federal registry records or by requesting documentation related to their incorporation from the client.

- 4 Ownership Disclosure:

1. Ownership details are self-reported by the client.

1.1. In cases where a client is categorized as high risk, the presentation of share certificates or a shareholder register may be solicited.

- 4.1.2 Any individual owning 25% or more of an organization is mandated to furnish, at a minimum, their full name and address.
- 4.1.3 Clients are also required to provide their date of birth, identity document particulars, and documentation validating their residential address.
- 4.1.4 Owners are provided with the opportunity to voluntarily disclose any affiliation with politically exposed persons, as well as the same disclosure option for their staff.

- 5 Watch List Screening:

5.1 Leveraging SUMSUB, entity names and ownership information are scrutinized against various watch lists, including the OFAC SDN (Office of Foreign Assets Control Specially Designated Nationals) and OSFI (Office of the Superintendent of Financial Institutions) lists.

2. In instances where a potential match is detected, additional information will be sought from the client, and enhanced due diligence procedures will be implemented.
3. MINTPAY LTD. does not knowingly engage in transactions with excluded parties.
4. Positive matches will result in a denial of service, while all other outcomes trigger enhanced due diligence measures and ongoing monitoring.

15. Customer Identification

The Know-Your-Customer (KYC) principle is a fundamental requirement for customer identification. This principle entails the identification of essential information, including the operational profile, purpose of operation, beneficial owner, and, if necessary, the source and origin of funds used in transactions, for potential customers. Additionally, other relevant information necessary for establishing a business relationship must be identified. In the course of conducting transactions, customer identification is essential. The compliance of transactions is assessed based on the customer's primary fields of activity and prior payment behavior. In

accordance with the risk-based approach, the Company selects the appropriate scope of the KYC principle, among other considerations.

The Company is required to identify the customer and the beneficial owner within a reasonable period before initiating steps to enter into a long-term contract or during contract initiation. Any person participating in a transaction must also be identified before taking steps to enter into a long-term contract or during contract initiation.

All information and documents related to the establishment of identity shall be securely preserved in a manner that facilitates a comprehensive and expeditious response to inquiries from the The Financial Transactions and Reports Analysis Centre of Canada (FINTRAC), investigative bodies, courts, or supervisory authorities. To achieve this, the Company shall implement a system capable of swiftly retrieving the necessary information or documentation pertaining to customer or transaction identification, considering the specific characteristics of its operations.

The identification and verification of individuals when establishing a business relationship are obligatory for all financial services, irrespective of whether a long-term contract is formed with the transaction participant. This consideration takes into account exceptions outlined in the Money Laundering and Terrorist Financing Prevention Act.

15.1.PERFORMANCE OF IDENTIFICATION

- The liable person shall identify the client:
- at the latest if it is clear that the value of the one-off transaction exceeds CAD 1 000
- always regardless of the limit set out above, in respect of:
- notwithstanding the limit laid down in paragraph 1, the liable person shall also always identify the client in respect of:
- Suspicious transaction:
- cash deposits followed by their immediate withdrawals or transfers to other accounts,
- freezing of accounts by one client, if their number is in a manifest disproportion to the subject of his business activity or his property relations, and transfers between these accounts,

- cases where the number of turnovers on the account during one day or in the following days does not correspond to the usual monetary operations of the client,
- transactions that clearly have no economic reason, cases where the participant in the transaction is directly or indirectly a legal or natural person against whom the Canada applies international sanctions under a special legal regulation (United Nations Act (R.S.C., 1985, c. U-2))
- cases where the subject of trade is, even if only in part, a service provided to a sanctioned entity or a sanctioned person
- Transactions directed to a country that does not apply anti-money laundering measures insufficiently or at all List of countries that do not apply anti- money laundering measures at all.
- cases where the subject of trade is, even if only in part, a service provided to a sanctioned entity or a sanctioned person (Special Economic Measures Act (S.C. 1992, c. 17))

Transactions directed to a country that does not apply anti-money laundering measures insufficiently or at all List of countries that do not apply anti- money laundering measures at all.

- 1 Identification of the Customer – Natural Person

1. The Company conducts the identification of natural person Customers, and when relevant, their representatives, and retains the following data on the Customer and their representative:

- Name(s) and surname(s)
- Personal number
- Citizenship
- Photograph
- Signature

2. The following valid identity documents that contain the specified data may serve as the basis for the identification of a natural person:

- An identity document of Canada
- An identity document of a foreign state
- A residence permit in Canada
- A driving license issued in a state of Canada, the USA, or the European Economic

Area

- 2 Identification of the Customer – Legal Entity

1. The Company performs the identification of Customers that are legal entities, along with their representatives, and retains the following data on the Customer:

• Business name or name
• Legal form
• Registration number (if issued)
• Name(s) and surname(s), personal number (in the case of a foreigner – date of birth or, if available, a personal number or any other unique sequence of symbols intended for personal identification) and citizenship of the director(s) or member(s) of the management director(s) of another equivalent body, along with their authorities in representing the Customer
• An extract of registration and its date of issuance
• Head office (address) and address of actual operation

2. For the identification of the Customer, documents issued by a competent authority or body not earlier than six months before their use may be accepted, including:

• Registry card of the relevant register
• Registration certificate of the relevant register
• A document equivalent to the aforementioned documents or relevant documents establishing the Customer.
• The accuracy of the Customer's data specified above is verified using information from a credible and independent source. If the Company has access to the relevant legal entity register, the submission of the specified documents is not required from the Customer.

The identity of a legal entity and the right of a legal entity's representation can be verified based on a document specified above, authenticated by a notary or certified by a notary or officially, or through other information originating from a credible and independent source. This process involves utilizing at least two different sources for data verification in such cases.

3. Natural person non-entrepreneur: finds out all names and surnames, birth number and, if not assigned, date of birth, place of birth, sex, permanent or other residence

and citizenship. The obligated person shall record and verify the data from the identity card (if they are stated in it), further record the type and number of the identity card, the state, or the authority that issued it and the period of its validity. At the same time, the liable person shall verify the conformity of the form with the image in the identity card;

4. Natural person entrepreneur: finds out all names and surnames, birth number and, if not assigned, date of birth, place of birth, sex, permanent or other residence and citizenship. The obligated person shall record and verify the data from the identity card, further record the type and number of the identity card, the state, or the authority that issued it and the period of its validity. At the same time, the liable person shall verify the conformity of the form with the image in the identity card. It is also necessary to record the name of the business company, distinguishing the appendix or other designation, the place of business and the identification number of the person;

4. Legal entity: finds out the name of the business company including the distinguishing appendix or other designation, registered office, identification number of the person or a similar number assigned abroad. The obligated person shall record and verify these identification data from the document on the existence of a legal entity, which is a valid extract from the Commercial Register. of this electronic OR or other business register. If the client is a legal entity registered in the trade register, download or check the data provided by the client orally or in a written communication. If it is a foreign legal entity, a valid extract from the business register must be submitted to the liable person in the original or a copy certified by an authorized authority, if it is not publicly available in a similarly verifiable form as currently extracts from the Commercial Register in the Canada.

The obligated person shall also identify the natural persons who act on behalf of this legal entity in the given business (or business relationship). In the case of natural persons who are members of the statutory body of this legal entity, but do not act within the scope of the business (or business relationship) in question, data for identification and verification are identified and recorded. These data are those that can be found from available sources, typically from the Commercial Register, ie in particular name, surname, date of birth and address. In the event that the client's

statutory body (or its member or controlling person) is another legal entity, the liable entity shall also record its identification data.

Trust fund or other legal arrangement without legal personality: finds out its designation and identification data of its administrator, manager or person in a similar position to the extent specified above, depending on whether they are natural or legal persons.

- To find out the **individual data:**

• Birth date;

• Gender: the information becomes more important especially for foreigners with names whose gender is not obvious (eg they do not contain the suffix -ová), or if it does not follow from the birth number;

• Place of birth: the format for recording the place of birth is not prescribed by AML by law, it should be clear and unambiguous. From the linguistic point of view, the "place" can probably not only be the state, but a real place concretized in a suitable way, ie for example a municipality + a state. If only the name of the municipality is recorded, from which it can be deduced that it is the territory of the Canada, it is probably unnecessary to write to the state as well. However, it will be necessary to be careful to use the name of the city, which appears in the same form in another state. On the other hand, for some people from a foreign state, it will be a problem to determine a specific place, if it is not mentioned in the personal documents. Then it will be practically impossible to record a more detailed determination of the place of birth than the state;

• Permanent or other residence: the indication of the relevant residence should be traceable and existing (possibility of verification on the Internet), while it should be verifiable in the relevant documents. Usually this means the house number (or apartment), street, village, state. So it is not enough just the name of the street and the house number, but it is also necessary to state the municipality. Postal code is not a condition, moreover, it is not used in all countries, or it can have a different format; on the other hand, its importance for clarification in the event of a likelihood of confusion is indisputable. If a person uses more than one address, it is advisable to record all of them.

• Authority that issued the identity card: this information must be recorded especially

in a situation where the client is a Canada national. In such a case, it is not expedient to record only the state that issued the identity card, as this card could not be issued when the client has dual citizenship and for the purpose of identification submits an identity card issued by a state other than the Canada).

15.2 Cryptocurrency Wallets Verification

1. Wallet Address Registration

Clients are required to register their cryptocurrency wallet addresses in the MINTPAY LTD. system.

In accordance with the company's requirements, the client must enter their wallet number in the designated field within their personal account on the platform.

2. Ownership Declaration

Clients must agree to the ownership declaration, which is available in their personal account.

When declaring ownership of the registered wallets, the client signs a form confirming that the provided information is accurate and up to date.

The client also confirms that they are the sole rightful owner of the crypto assets in the registered wallets.

3. Sanctions Screening of Cryptocurrency Wallets

All registered cryptocurrency wallets are subject to screening against established sanctions lists and blacklists.

This is necessary to ensure compliance with regulatory standards and prevent illegal activities related to money laundering and terrorism financing.

4. Monitoring and Reporting

All information regarding registered wallets and transactions will be regularly reviewed for anomalies and discrepancies.

We use advanced blockchain analytics tools, such as those provided, to monitor transaction history and detect suspicious patterns. For crypto transaction monitoring, we use AMLBot (https://amlbot.com/ru/certifications) and conduct internal transaction analysis with our in-house AML specialists.

Monitoring is performed for every crypto transaction without exception.

AMLBot analyzes the following risk sources:

- Child Exploitation: Entities involved in child exploitation.
- Dark Market: Coins associated with illegal activities.
- Dark Service: Coins linked to child abuse, terrorism financing, or drug trafficking.
- Enforcement Action: Legal entities facing legal proceedings.
- Fraudulent Exchange: Exchanges involved in exit scams, illegal activities, or whose funds have been seized by authorities.
- Gambling: Coins linked to unlicensed online gambling.
- Illegal Service: Coins associated with unlawful activities.
- Mixer: Coins passed through a mixer to obscure or make tracking impossible, often used for money laundering.
- Ransom: Coins obtained through extortion or blackmail.
- Sanctions: Entities under sanctions.
- Scam: Coins obtained through fraudulent schemes.
- Stolen Coins: Coins obtained by stealing another party’s cryptocurrency.
- Terrorism Financing: Entities involved in the financing of terrorism.
- In the event of detecting suspicious activity, our company acts in accordance with regulatory requirements and FINTRAC guidelines.

5. Policy Compliance

If suspicious activity is detected, the wallet will be flagged for immediate review. All flagged transactions will undergo additional manual analysis to determine if they are linked to illegal activities, such as fraud, ransomware, or theft.

If there are grounds to classify a transaction as suspicious, MINTPAY LTD.'s AML team takes the following actions:

Blocks the incoming funds.

Reviews the client's activity (verifying their identification data and transaction history).

Prepares a Suspicious Transaction Report (STR) and submits it to FINTRAC in accordance with the procedure outlined in Paragraph 36 of this policy.

Conducts an internal investigation to determine the cause of the suspicious activity and implements measures to prevent future occurrences.

6. Staff Training

All company employees involved in the wallet verification process undergo regular AML training, which includes guidelines on identification and risk management. See more in Paragraph 38.

16. Required types of identity card

ID card, passport, driver's license, foreigner's residence permit, firearms license, etc.

The following types of identity cards may be accepted only if they meet the following requirements:

- it is a valid document issued by the state;
- it is not a card damaged above the usual level of wear (eg missing sheets, glued, overwritten, illegible, etc.);
- the image of the holder on the card must correspond to the actual form of the holder and must be clear or undamaged enough to allow the holder to be identified with a sufficient degree of probability;
- it is a document from which it is possible to determine which authority of which state issued it;
- it is a document which, for whatever reason, does not raise doubts as to its arbitrariness.

Some identifying information (eg gender, residence address) may not be included on every identity card. Such data can be found, for example, only on the basis of a statement identified, but preferably from another supporting document. Here, the liable person determines his own measures whether the client's statement will suffice or whether the missing data will be required to be documented by type of document, for example according to the nature of the transaction or according to the type of client.

The liable person may make copies or extracts from the submitted documents and process the information thus obtained for the purposes of the AML Act. Making copies of personal documents as part of personal identification is only possible with the consent of the holder.

If, at the conclusion of the transaction (or business relationship), the liable person

suspects that the client is not acting on his own behalf or that he is concealing that he is acting on behalf of a third party, he shall invite the client to provide the original or a certified copy of the power of attorney. Everyone is obliged to comply with this challenge.

17. Other identification options

In addition to the identification performed in the physical presence of the client, the liable person uses these other options when performing the identification of the client.

Identification of the client represented on the basis of a power of attorney

The identification of the proxy is performed (as well as the identification of the natural person, see above), the necessary submission of the original or a certified copy of the power of attorney with the officially certified signature of the principal. The agent shall provide the identification data of the represented party.

Identification of the client represented by the legal representative or guardian

The identification of the proxy is performed (as well as the identification of the natural person, see above), it is necessary to submit the original or a copy of the power of attorney with the officially certified signature of the principal. The agent shall prove the identification data of the principal, personal delivery of a copy of the identity card of the represented person or we accept the provision of data on the power of attorney.

The identification of the legal representative or guardian is performed (as well as the identification of the natural person, see above). The legal representative shall document the identification data of the represented party, the guardian shall also submit the relevant decision of the court on his / her appointment, resp. reference number of this decision. The legal representative is obliged to personally deliver a copy of the identity card or court decision.

All data are recorded in the questionnaire "Record of meetings" of MINTPAY LTD., which is filled in in accordance with the requirements of the FINTRAC and AML.

18. Identification of Politically Exposed Persons (PEPs)

- 1 Definition of Politically Exposed Persons (PEPs):

• PEPs refer to natural persons who currently hold or have previously held significant public positions and their immediate family members or close associates.

- 2 Prominent Public Functions Include the Following:

• Head of state, head of government, minister, vice-minister, deputy minister, secretary of state, chancellor of parliament, government, or ministry.

• Member of parliament.

• Member of the Supreme Court, Constitutional Court, or other supreme judicial authorities with final decision-making authority.

• Mayor of a municipality or head of a municipal administration.

• Member of the management body of the supreme institution of state audit or control, or chair, deputy chair, or member of the central bank board.

• Ambassadors of foreign states, chargé d'affaires ad interim, heads of the armed forces, commanders of armed forces and units, chief of defense staff, or senior officers of foreign armed forces.

• Member of the management or supervisory body of a public undertaking, public limited company, or private limited company, where more than half of the total votes at the general meeting of shareholders are owned by the state.

• Member of the management or supervisory body of a municipal undertaking, public limited company, or private limited company where more than half of the total votes at the general meeting of shareholders are owned by the state, and they are considered large enterprises under the Law on Financial Statements of Entities of the Canada.

• Director, deputy director, or a member of the management or supervisory body of an international intergovernmental organization.

• Leader, deputy leader, or a member of the management body of a political party.

- 3 Close Family Members Include:

• Spouse or partner with a registered partnership (cohabitant).

• Parents.

• Siblings.

• Children and children's spouses or cohabitants.

- 4 Close Associates Are Defined As:

• A natural person who shares membership in the same legal entity or an unincorporated body or maintains another business relationship with the Politically Exposed Person.

• A natural person who is the sole Beneficial Owner of a legal entity or unincorporated body established or operating de facto to acquire assets or other personal benefits for the Politically Exposed Person.

- 5 PEP Identification Procedures:

• The Company employs measures to determine whether the customer, their beneficial owner, or their representative holds PEP status, is a family member or close associate of a PEP, or has become one. These measures include:

• Inquiry during customer onboarding.

• Reference to publicly available information.

• Screening relevant individuals against commercially available databases to establish PEP status.

- 6 Monitoring of Former PEPs:

• In cases where a customer with PEP status no longer holds prominent public functions, the Company shall, at a minimum, for 12 months, consider the remaining risks associated with the customer. It will implement relevant risk-based measures until it is certain that the typical risks associated with PEPs no longer apply to the customer.

MINTPAY LTD. conducts continuous monitoring of Politically Exposed Persons (PEP) accounts in compliance with updates in PCMLTFA, SOR/2023-194, provide mandatory monitoring for all PEP accounts for a minimum of 36 months after their political functions have ceased.

Conduct periodic reviews of PEP accounts every six months (PCMLTFA, SOR/

2023-195).

Enhanced due diligence procedures include collecting information on the client's ties to public positions, family members, and close associates, as defined in Sections 9 and 11 of PCMLTFA. We also commit to implementing additional controls to mitigate risks associated with these financial activities.

19. Source of Wealth and Funds

Establishing the Customer's source of wealth (SoW) and source of funds (SoF) is a core requirement of EDD.

Source of Wealth (SoW) Defined:

- SoW refers to the origin of the customer's entire body of wealth (i.e., total assets). SoW explains activities the customer participates in and their geographical location. This information will usually give an indication as to the volume of wealth the customer could be expected to have, and a picture of how the customer acquired such wealth. When establishing SoW, there is no need to establish funds used in a specific transaction. The goal of SoW establishment is to understand and verify that the customer's SoW corresponds with data given by the Customer when onboarding, and the volume of the customer's wealth allows them to perform transactions with the expected turnover specified by the customer.

Source of Funds (SoF) Defined:

- It is necessary to find out the source of the funds used in the trade or business relationship. In the case of a business relationship, this part of the client's control is performed especially when it arises, obtaining the so-called input information.
- It is necessary to obtain input information at least to such an extent that you will subsequently be able to assess during the business relationship whether the individual transactions are actually related to the client's business or usual income, whether they correspond to his normal activities, etc. In order to make such an assessment, it is appropriate find out whether the client is an employee, pensioner, student, etc. Furthermore, for example, an indication of the expected amount of the transaction.
- If the funds come, for example, from business activities, it is necessary to specify

which business activity it is.

- Other sources of money can be, for example, gifts, inheritances, wages. [In case of doubts of the liable person about the veracity of the information obtained about the client, or if, for example, the client is categorized as risky, it is appropriate to prove the source of funds by evidence, such as invoice, contract for sale of real estate, resolution to inherit, etc.
- SoF refers to the origin of funds being deposited, received, or transferred with the Company. SoF tells where the assets are coming from, which can be proven through bank statements, tax returns, or the customer's financials, etc. Typically, SoW is requested when establishing a business relationship or performing EDD, SoF is requested when there is a need to understand what the origin of a transaction is.

Verification of SoW and SoF:

- The types of data and documents that can be used for verification will vary depending on the circumstances and the information that the customer provides to the Company. The Company collects information relating to SoW or SoF of its customers and, according to the level of risk involved, takes reasonable steps to verify that information.
- The following documents, data, or information could be considered reliable and independent:
- Government-issued or registered documents or data;
- Full bank and other investment statements;
- Full payslips or wage slip or other documents confirming salary;
- Inheritance (stamped grant of probate, stamped grant of letters of administration);
- Audited financial accounts from a chartered accountant or Charities Services;
- Letter from an agent of the customer confirming they have knowledge of and established business relationships with the customer;
- A copy of a will;
- Sales and purchase agreements.

Verification of Funds for Business Transactions:

- For customers who conduct their business with Company, there is a range of documents that Company can use to verify how funds have been acquired (e.g.,

balance statements and other accounting documents, contract with counterparties, invoices, proof(s) of work, etc.).

Transaction Volume Limits:

- The company establishes limits on the volume of transactions, after which the source of funds must be requested, in the requirements for transactions monitoring.

20. The establishment of a business relationship and client control

Procedures for performing client control, determining the scope of client control corresponding to the risk of money laundering and terrorist financing

By performing a client check, the liable person obtains the information he needs to assess whether or not the transaction is suspicious. The information obtained about the client, his business and other activities should be relevant to the business and services that the client requests from the liable person and should provide sufficient information to assess the client's risk.

MiCA

MINTPAY LTD.. implements transparency measures required by the MiCA regulation (Regulation (EU) 2023/1112, dated June 9, 2023), including mandatory disclosure of the Source of Funds (SoF) and blockchain transaction monitoring procedures. All transactions exceeding €10,000 are logged and verified under MiCA and PCMLTFA compliance guidelines.

Cross-Border Transactions:

Under the Markets in Crypto-Assets Regulation (MiCA) (Regulation (EU) 2023/1114, effective June 29, 2024), the company must:

Maintain detailed records of virtual asset transactions exceeding €1,000, including sender and recipient identification, wallet addresses, and IP addresses (MiCA, Article 61).

Regularly update KYC information for all cryptocurrency service users.

The liable person always checks the client:

Before the trade takes place outside the business relationship, at the latest when it is clear that it will reach a value of $ 10,000 (in any equivalent currency. including in virtual currency) in accordance with PCMLTFR SOR/2002-184, ss. 84(b), 105(7)(a), 109(4)(a) and 112(3)(a).). The obligation to control the client also applies in the case of a transaction with a politically exposed person.

* This obligation is subject to the 24-hour rule.

- Large cash transactions
- Large virtual currency (VC) transactions
- Suspicious transactions
- Issuing or redeeming traveller's cheques, money orders, or similar negotiable instruments of $3,000 or more
- Transmitting $1,000 or more in funds by means other than an electronic funds transfer (EFT)
- Initiating an EFT of $1,000 or more
- Foreign currency exchange transactions of $3,000 or more
- Transferring VC in an amount equivalent to $1,000 or more
- Exchanging VC in an amount equivalent to $1,000 or more
- Remitting funds in the amount of $1,000 or more to a beneficiary, by means other than an EFT
- Remitting funds to the beneficiary of an international EFT of $1,000 or more
- Remitting VC to a beneficiary in an amount equivalent to $1,000 or more
- Information records
- Crowdfunding platform donation (PCMLTFR, SOR/2002-184, ss. 95(1)(h), 95(3)(c) and 95(4)(c).)
- On obtaining information on the purpose and intended nature of the business or business relationship on determining the beneficial owner, if the client is a legal entity
- on obtaining information necessary to conduct ongoing monitoring of the business

relationship, including reviewing business during the relationship to determine whether in accordance with what the liable entity knows about the client and his business risk profile about reviewing sources of funds.

- with PEP;
- with a person established in a country who is to be considered as at high risk on the basis of a designation from the European Commission or for some other reason. This is a person who has the nationality, residence (permanent or temporary), registered office, branch or organizational unit in the so-called country at risk;
- before the suspicious transaction takes place;
- the establishment of a business relationship (at the latest before the first transaction);
- when concluding a safe deposit box lease agreement or custody agreement (at the latest before the first transaction takes place);
- during the business relationship;

If a transaction is divided into several separate transactions, the value of the transaction is the sum of those transactions, if they are related. Obviously related transactions must therefore be added together and regarded as a single transaction.

Client control includes:

- obtaining information on the purpose and intended nature of the trade or business relationship;
- ascertaining the ownership and management structure of the client and its beneficial owner, if the client is a legal entity, trust or other legal arrangement without legal personality, and taking measures to identify and verify the identity of the beneficial owner;
- continuous monitoring of the business relationship, including a review of the transactions carried out during the relationship in order to determine whether the transactions are in accordance with what the obligated person is aware of about the client and his business and risk profile;
- examining the sources of cash or other assets to which the business (or business relationship) relates;
- in the context of the business relationship with PEP, also appropriate measures to determine the origin of its assets.

20.1. Obtaining information about the purpose and intended nature of the business or business relationship

The purpose of obtaining this information is to create conditions for future evaluation of whether sub-transactions show signs of suspicious trade.

The information obtained by the liable person must be in such a volume that it is possible to assess the client in terms of the possible risk of ML / FT. The volume of information obtained at this point also varies depending on the type of liable person.

Obtaining information about the client's ownership structure and finding out the client's real owner is necessary for the client's assessment in terms of possible ML/FT risk.

The liable person ascertains the relevant relations up to a specific natural person or more natural persons who have a significant influence on the activities of the given client, even indirectly (through other natural or legal persons).

In order to know the real owner, it is necessary to take measures in order to understand the ownership and management structure of the client, ie. obtaining information on its status, shareholders and governing bodies. If the beneficial owner is listed in a public register and you have no doubts about the accuracy and timeliness of this information, this source of information and a link to it will suffice. Otherwise, it is necessary to take reasonable steps to determine the current situation, while it is possible to use the client's obligation to cooperate according to § 9 paragraph 7 of the AML Act. (PCMLTFR SOR/2002-184, ss. 88(a)(i), 88(b)(i) and 88(c)(i).)

During the inspection of the client - legal entity, the liable person finds out and records:

- for the beneficial owner, information to verify his identity and the procedure for identifying him.
- when determining appropriate authentication measures, you should take into account the ML / FT risk posed by the client and the business relationship with him. In general, information should suffice for this purpose to the extent that it is usually published in business registers, for example with the statutes of business corporations. The minimum of such data can be considered as finding out the name,

surname, address, country of origin of the real owner and a description of the relationship with the client. If the relevant data can be supported by documents, it may be recommended that copies be kept and kept, or that a reference to the relevant database be recorded.

- in the case of an intended trust fund or other legal arrangement without legal personality, see the provisions of PCMLTFR SOR/2002-184, s. 89(a)., (PCMLTFR SOR/2002-184, ss. 89(e)(i) and (ii).) of the AML Act When performing a client inspection, the liable entity shall ascertain and record at:

a) the beneficial owner of the data to verify his identity and the procedure for identifying him,

b) an intended trust or other legal arrangement without legal personality, which is determined on the basis of certain characteristics or belonging to a certain category, information sufficient to identify a particular intended person at the time of payment of proceeds or at the time when the intended person exercises his acquired rights,

c) beneficiaries of life insurance which is.

• determined as a specific person or legal arrangement without legal personality, his name and surname or name,

• determined on the basis of his relationship with the insured or otherwise, information sufficient to identify a specific entitled person at the time of payment of benefits,

• a politically exposed person, all significant circumstances and the course of the business relationship. The determination of the beneficial owner is also carried out during the business relationship so that the periodicity of inspections covers all changes that have occurred.

• After finding out the real owner and ownership structure, it is necessary to check whether the persons thus identified are not on the list of sanctioned entities.

Concluding a contract for renting a safety deposit box or a contract for safekeeping, purchase or acceptance of cultural monuments, objects of cultural value, second-hand goods or goods without proof of its acquisition to mediate their sale or acceptance of pledges, or payment of the balance of the canceled deposit from the passbook to the

bearer.

20.2.CLIENT CONTROL INCLUDES:

- obtaining information on the purpose and intended nature of the business or business relationship to establish the beneficial owner, if the client is a legal entity
- obtaining the information necessary to carry out ongoing monitoring of the business relationship, including a review of the transactions carried out during the relationship to determine whether the trades are in line with what the obligor knows about the client and his business risk profile.
- It is clear that the fulfilment of the above points is easily formally achievable, but the actual fulfilment, eg finding the owner of a joint stock company, is often unsatisfactory for the insurance intermediary (and not only for him). Therefore, the fulfilment of this task is expected in cooperation with the executive.
- Trust fund or other legal arrangement without legal personality: finds out its designation and identification data of its administrator, manager or person in a similar position to the extent specified above, depending on whether they are natural or legal persons.

Procedures in case of not finding the real owner

- There are situations where the real owner cannot be identified. In particular, the following cases apply: the real owner cannot be identified because, forexample, he is hidden behind companies registered in the state, which allows to hide their ownership structure and the client does not know the persons who manage or control these companies. If in such a case the client does not submit at least a solemn declaration or otherwise proves his ownership structure, the liable person will not carry out the transaction or establish a business relationship.

- the real owner is determined only from the client's statement, which cannot be independently verified. In such a case, this fact must be adequately reflected in the risk profile and appropriate measures must be taken againstit in accordance with the established rules. liable persons (this may be an unclear ownership structure and therefore needs to be adjusted).

- the liable person may, when determining the real owner of the client, conclude that no such person exists. In that case, it is necessary to state as the real owner the natural person or persons who perform the highest management function at the client (ie, actually exercise a decisive influence on the management of the company, ie, for example, members of the statutory body). If such information cannot be substantiated by an official document, then it must be substantiated by a written statement of the responsiblerepresentative of the client;

the client does not provide cooperation, or there are doubts about the veracity or reliability of the information provided. For, this behavior is a reasonto refuse to trade.

21. Appointment of liable person

Statutory Requirement: The Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA) mandates the appointment of a liable person responsible for overseeing the company's compliance regime.

Independent Oversight: The liable person operates autonomously, without any direct reporting obligations to other company departments or divisions. They hold a direct reporting line to the executive team, ensuring impartiality and robust oversight of anti-money laundering activities.

- Duties and Responsibilities: The liable person duties encompass a broad spectrum of responsibilities, including but not limited to:

• Administration and Implementation of Risk Management Policies: The liable person is tasked with administering and executing the risk management policies of MINTPAY LTD.. on a comprehensive basis.

• Risk Assessments: Conducting Anti-Money Laundering (AML) risk assessments of new markets, industries, and clients as necessitated by the business operations.

• External Partnerships Review: The Compliance Officer is responsible for evaluating external partnerships with vendors, acquirers, and other parties to ensure alignment with MINTPAY LTD..'s risk appetite, brand, and policies.

• Regulatory Monitoring: Continuous monitoring of regulations in major jurisdictions and industries where MINTPAY LTD.. and its clients conduct business, with a focus on identifying material changes.

- Policy Maintenance: Ensuring that the company's Anti-Money Laundering (AML) policy suite remains up to date and compliant with industry and market regulations.
- Risk Mitigation: Conducting periodic risk assessments and implementing measures to mitigate, avoid, or transfer risks as necessary.
- AML Training: Facilitating anti-money laundering (AML) training for all staff members to enhance awareness and compliance.
- Ongoing Monitoring: Engaging in ongoing monitoring of transactions and the reputation of MINTPAY LTD. and its clients to identify and respond to suspicious activity.
- Independent Reviews: Coordinating and facilitating periodic independent reviews of the company's compliance regime to ensure its effectiveness and adherence to regulatory standards.
- Responding to Requests: Addressing requests for information from law enforcement, regulatory bodies, and external parties in response to third-party inquiries.
- Reporting to Management: Providing regular reports to the company's management on compliance activities and the overall status of the compliance regime.
- Information Disclosure: Responding to requests from regulatory authorities for information regarding corporate structure, ownership, and licensing from suppliers.
- Delegation: The liable person has the authority to delegate any of the aforementioned tasks or related responsibilities to junior Compliance staff, overseeing their execution and completion.

21.1.Contact person

The contact person is Tyler Jade Egginton, CEO.

22. Investigation Unit

- Investigation Unit works under the auspices of the AML Officer. The following functions shall be performed by the Investigation Unit:
- Assistance of the AML Officer regarding reviewing received internal disclosures

and exception reports.

- Assistance of the AML Officer regarding filing reports to the FINTRAC.
- Perform other functions assigned to the Investigation Unit under the internal policies and job description.

- Audit Function

- Audit function shall be established to perform regular reviews of the AML/CTF systems to ensure their effectiveness. The frequency and extent of the review should be commensurate with the risks of ML/TF and the size of the Company's business, as well as regulatory requirements. Where appropriate, the Company will seek a review from external auditors.
- Independent audit functions include the following principles:
- Compliance and audit functions are independent in practice.
- The regular review is performed at a frequency of at least once in 1 year.
- External parties are leveraged to perform the auditing.
- Availability of direct communication to senior management through regular committees (compliance committee) or other means of direct communication.

23. Risk-Based Approach (RBA)

An RBA is a way for you to conduct your risk assessment by considering elements of your business, clients and/or business relationships to identify the impact of possible ML/TF risks, and to apply controls and measures to mitigate these risks.

The Financial Action Task Force (FATF), has developed a series of Recommendations that are recognized as the international standard for combating money laundering, terrorism financing and other related threats to the integrity of the international financial system. Recommendation 1 on the RBA, recognizes that an RBA is an effective way to combat money laundering and terrorist financing.

- Adherence to the Risk-Based Approach:

By adopting a risk-based approach, the Company ensures that measures to prevent or mitigate Money Laundering (ML) and Terrorist Financing (TF) threats are commensurate with the risks identified. This efficient allocation of resources focuses on the highest-priority risks, allowing for effective risk management.

- Inherent Risk Assessment:

In the process of identifying specific products, services, customers, entities, and geographic locations, the inherent risk is assessed. Not all risks are uniform; they vary based on the characteristics of the particular product, service, or customer. Factors such as transaction volume, geographic location, and the nature of customer relationships are considered.

- Customer Risk Profile:

During the on-boarding stage of a new customer, risk assessment provides insight into the potential customer's type, geographic location, and business activities. Ongoing determination of the customer's risk profile ensures that the appropriate risk level is assigned throughout the established relationship.

- Tailored Due Diligence Measures:

The Company utilizes a risk-based approach (RBA) to determine the extent of Customer Due Diligence (CDD) measures and ongoing monitoring. These measures are customized based on the customer's background and the product, transaction, or service they are using. This ensures that preventive and mitigating measures are proportionate to identified risks.

- Key Aspects of the RBA:

The RBA enables the Company to subject its customers to proportionate controls and oversight by determining:

• The extent of the due diligence to be performed on the direct customer.
• The extent of the measures to be undertaken to verify the identity of any beneficial owner and any person purporting to act on behalf of the customer.
• The level of ongoing monitoring to be applied to the relationship.
• Measures to mitigate any identified risks.

- Managing ML/TF Risks:

An RBA involves identifying and categorizing ML/TF risks at the customer level and establishing reasonable measures based on these identified risks. The RBA does not discourage the Company from engaging in transactions with customers or establishing business relationships with potential customers. Instead, it assists the Company in effectively managing potential ML/TF risks.

Risk Assessment

The obligated person identifies and assesses the risks of money laundering and terrorist financing, which may occur within the scope of its activities subject to the scope of this Act. When assessing risks, the liable entity shall also take into account the factors of possible higher risk, listed in Assessment of Inherent Risks of Money Laundering and Terrorist Financing in Canada: (https://www.canada.ca/en/department-finance/services/publications/assessment-inherent-risks-money-laundering-terrorist-financing.html)

The obligated person referred to in § 2 par. 1 let. (a) to (d) and (h) draw up, no later than 60 days from the date on which he became liable, a written assessment of the risks of money laundering and terrorist financing for the types of trade and commercial relations provided, to the extent that he carries out activities subject to scope of this Act. It shall take into account risk factors, in particular the type of client, the purpose, regularity and duration of the business or non-business business, the type of product, the value and manner of the business and the riskiness of the countries or geographical areas to which the business relates.

The risk assessment pursuant to paragraphs 1 and 2 also includes measures for internal control, control of compliance with legal regulations and verification of the liable person's employees and according to the scope and nature of the liable person's activities also the establishment of an independent unit for testing these measures, strategies and procedures according to § 21 par. 1.

The obliged entity shall regularly update the risk assessment pursuant to paragraph 2, in particular before the start of the provision of new products.

Obliged persons who are part of a group shall apply group strategies and procedures to combat money laundering and terrorist financing, including data protection procedures to the extent permitted by the law of a third country and strategies and procedures for information sharing within the group. Those strategies and procedures shall also apply to branches and subsidiaries in other The risk assessment must include at least:

• risk categorization of client types with regard to risk factors;

• risk categorization of products and related services that can be misused to ML / FT;

• exemplary (not statutory and generally formulated) signs of suspicion that could indicate suspicious behavior, suspicious transaction patterns, etc. for individual types of clients; The suspicion features described in this way must be the result of the portfolio of products and services provided. The following must also be included in the above minimum content: - country risk factor.

24. Risk profiles

In the risk assessment, the liable person may draw, inter alia, from the following information:

• from the approved report on the first round of the ML / FT national risk assessment process (this report is distributed by the FINTRAC in a controlled manner);

• from own analysis of previously submitted STR;

• numerous analyzes can be found on the website www.fatf-gafi.org, which are focused both by sector and typology.

MINTPAY LTD.., identifies and assesses the risks of Money Laundering and Terrorist Financing that may arise in the course of its activities subject to the AML Act. When assessing risks, the company will also take into account the factors of possible higher risk, listed in Annex No. 2 to this internal regulation. MINTPAY LTD... creates a written risk assessment of Money Laundering and Terrorist Financing (hereinafter "Risk Assessment") for the types of brokered transactions and business relationships to the extent that it carries out activities subject to the AML Act.

25. Risk Categories

The Company conducts regular risk assessments to identify, analyze, and manage Money Laundering (ML) and Terrorist Financing (TF) risks. The risk assessment process, integral to the Risk-Based Approach (RBA), encompasses the following stages:

• Risk Factors Identification: Identifying risk factors associated with ML and TF.

• Risk Factors Analysis: Analyzing these identified risk factors.

• Risk Factors Evaluation: Evaluating the risks posed by these factors.

- The Company relies on various sources during the risk assessment process, including but not limited to:

• Applicable regulatory requirements, including Canadian laws, the Proceeds of

Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA), Office of the Superintendent of Financial Institutions (OSFI) guidelines, Financial Action Task Force (FATF) orders, and more.

- The latest national risk assessment.
- Guidance provided by regulatory authorities, including international organizations.
- Knowledge derived from past experiences and activities akin to those of the Company.

- The Company assesses the ML/TF risks associated with its customers by assigning ML/TF risk ratings, taking into account the following risk categories:

- Customer Risk Factors (PCMLTFR, SOR/2002-184, s. 156(1)(c)(i).): These factors pertain to the customer's or their beneficial owner's characteristics, behavior, and other relevant circumstances. When identifying risk factors in this category, the Company considers:

- The customer's legal status, such as being an entity listed on a regulated market, a governmental authority, or an entity regulated by public law, credit or financial institution.
- The customer's Politically Exposed Person (PEP) status and any known connections to PEPs, including family members and close associates.
- The complexity of the customer's organizational structure, which includes the use of corporate structures, trusts, nominee directors/shareholders, and bearer shares.
- Any negative information about the customer or related persons, such as adverse media, warnings from regulatory bodies, or criminal records.
- The customer's behavior and personal attributes, including their education, knowledge in a particular field, and age.
- The customer's area of business activity, such as cash-intensive operations or other businesses vulnerable to ML or TF.
- The origins of the customer's wealth and the ability to verify its legitimacy.

- Country or Geographic Region Risk (PCMLTFR, SOR/2002-184, s. 156(1)(c)(iii).): These risk factors are associated with the jurisdiction or region where the customer is based. When identifying risk factors in this category, the Company examines whether the relevant country meets specific criteria related to jurisdiction and region, including:

• Being located in Canada, the European Economic Area, or the USA.
• Having been identified by the FATF as a jurisdiction with strategic AML/CTF deficiencies.
• Being subject to sanctions, embargoes, or similar measures issued by Canada, EU and UN.
• Having the status of a high-risk third country as defined by the relevant EU regulation.
• Being vulnerable to corruption or other criminal activity.
• Believed to have strong links to terrorist activities.

- Product and/or Services Risk (PCMLTFR, SOR/2002-184, s. 156(1)(c)(ii).): These factors relate to the specific services provided, including the volume of services, transaction patterns, and other elements that may impact the risk of ML or TF occurring during service provision. When identifying risk factors in this category, the Company considers:

• The volume of products and/or services requested or provided.
• Specific transaction patterns, including indicators of suspicious activity identified by FATF (Red flags).
• The intended purpose of the product and/or service, as well as any identified purposes.
• The potential use of the product and/or service in activities vulnerable to ML or TF and illicit (prohibited) activities.
• Ways in which the product and/or service may promote anonymity.

- Delivery/Distribution Channel Risk (PCMLTFR, SOR/2002-184, s. 156(1)(c) (ii).): These risk factors concern the channels used to provide services, encompassing identity verification methods, transaction execution, and authentication procedures. When identifying risk factors in this category, the Company takes into account:

• The method used to verify the customer's and its representative's identity, such as face-to-face meetings, remote verification, or the use of qualified electronic signatures.
• The credit institutions, financial institutions, paying institutions, or payment channels used by the customer.
• IP addresses and device IDs used by the customer.

- The use of solutions that enhance anonymity, such as VPNs, encrypted email, TOR browsers, one-time wallets, and similar technologies.
- The systematic assessment of these risk categories is crucial in enabling the Company to effectively manage and mitigate ML and TF risks as part of its compliance and risk management framework.

26. Distribution channel factor

MINTPAY LTD.. based on the information obtained during the identification and control of the customer, determines the risk profile of the customer. The Company always compiles and evaluates the risk profile with regard to at least the following risk factors:

a) the fact that one of the countries of origin of the customer, the person who acts with MINTPAY LTD.on behalf of the customer, or one of the countries of origin of the real owner of the customer is a state that insufficiently or not applies measures against Money Laundering and Financing terrorism, or by the state, which MINTPAY LTD. considers it risky based on its assessment;(b) the fact that, according to the information available to MINTPAY LTD. available, the subject of the trade was or is to be transferred or provided in connection with the trade from a state that insufficiently or not at all applies measures against Money Laundering and Terrorist Financing, or from a state that MINTPAY LTD. considers based on its assessment considered risky, or that the object of the trade was or is to be transferred or provided to such a state in connection with the trade;

c) the registration of the customer, the person who acts with MINTPAY LTD. on behalf of the customer, the real owner of the customer, the person with whom the customer carries out business, or if MINTPAY LTD. known to the final recipient of the object of the trade or the beneficial owner of the person withwhom the customer is carrying out the trade, on the list of persons and movements against which sanctions are applied in accordance with otherlegislation;

d)Opaque ownership structure of the customer;

e) unclear origin of the customer's funds (the customer declares the origin of the funds, eg as winning cash in a casino, receiving a gift - cash, obtaining an inheritance, etc.);

f) facts giving rise to suspicion that the customer is not acting on his own account or that he is concealing that he is complying with a third party's instruction;

g) the unusual way of conducting the business, especially with regard to the typeof customer, his current business activity, the subject, amount and method of settlement of the business, the purpose of the business relationship and the subject of the customer's activity;

h) facts indicating that the customer is conducting a suspicious transaction;

i) the fact that, according to the information available to MINTPAY LTD., the subject of the customer's activity is associated with an increased risk of Money Laundering or Terrorist Financing.

When establishing a business relationship with the customer, as well as during it, and when conducting transactions that are not part of the business relationship:

a) ascertains and stores such information about the customer that will enable it to evaluate whether it is a risky customer,

(b) checks the validity and completeness of customer data and updates it; and (c) pays increased attention to transactions (risk circumstances):

- in which there is any of the risk factors described above,
- performed with natural persons as part of services based on an individual approach to the customer, while these services are provided by MINTPAY LTD. only to those customers who meet special conditions set by the institution,
- politically exposed persons,
- for whom the institution is known that the real owner of the customer is a politically exposed person or that a politically exposed person otherwise participates in them, or. a large volume or high level of complexity, especially with regard to the type of customer, subject , the amount and method of trade settlement, the purpose of the business relationship and the subject of the customer 's activity.

27. Maintaining the Customer's Risk Profile

The Company reviews the business relationship with each customer as per the schedule below to ensure if the risk profile determined is still applicable or should be modified based on any changes of the identity of the customer, the nature of the customer's business, the customer's country of residence, the actual volume of transactions and other facts, which may affect the customer's risk assessment. Only the AML Officer is permitted to alter a customer's risk profile. The AML Officer will maintain relationship opening documentation, activity statements, and other necessary documentation to support the risk profiles assigned to customers.

1.Low Risk:

In the case of low-risk customers, the AML Officer is tasked with conducting annual reviews for each low-risk customer. These reviews involve an evaluation of the customer's risk profile and transactional activity to ensure ongoing compliance with anti-money laundering (AML) regulations and company policies.

2.Medium Risk:

For medium-risk customers, the AML Officer undertakes annual reviews of each medium-risk customer, with the condition that the customer is no longer in a new relationship. This entails conducting reviews every six months following the customer's initial onboarding. These reviews assess the customer's continued adherence to AML and due diligence requirements.

3.High Risk:

Given the elevated risk associated with high-risk customer relationships, the AML Officer is responsible for conducting regular reviews of every high-risk customer. These reviews encompass a thorough examination of the customer's transactional activity. Moreover, each high-risk customer necessitates Enhanced Due Diligence (EDD) before the commencement of the relationship. During this process, additional information and facts are gathered to gain a deeper understanding of the customer's risk profile.

4.For any non-individual customer whose business has been classified as a "high-risk business," the AML Officer is obligated to go a step further by independently verifying the existence of the business and the purpose of the business relationship

with the Company. This additional level of scrutiny is a crucial component of managing the inherent risks associated with high-risk customers and their business activities.

28.Enhanced measures required when working with high-risk clients

NOTIFICATION OF BUSINESS CONTACTS LIMITATION WITH CLIENTS FROM HIGH-RISK INDUSTRIES

MINTPAY LTD.. (hereinafter referred to as the "Company") aims to restrict its business contacts with clients from high-risk industries. However, there are certain exceptions within which commercial activities are permissible under specific circumstances.

Types of products and services considered unfair, predatory, or deceptive:

- Sales of online traffic or engagement

Regulated industries:

- Investment and brokerage services
- Money transmitters, currency exchange services, and other money services businesses
- Neobanks / challenger banks
- Other financial institutions
- Network marketing and referral marketing programs

In accordance with the Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations (PCMLTFR), SOR/2002-184, s. 157, additional measures are applied to clients from the above-mentioned categories. These measures include enhanced Know Your Customer (KYC) checks for directors, responsible persons, and ultimate beneficiaries. In addition to assessing electronic verification systems, additional checks are manually conducted by AML department specialists:

- Obtaining additional information about the client from publicly available databases and the internet.
- Gathering information about the source of funds or wealth of the client.
- Obtaining information about the reasons for attempting or conducting

transactions.

- Applying any other measures deemed appropriate by MINTPAY LTD..

Verification is required when establishing commercial relationships, and the source of funds check is requested for transactions amounting to $10,000 or more in any equivalent currency. Enhanced supervision of transactions is conducted, ensuring the update of client identification information and beneficial ownership information at a frequency corresponding to the risk level, specifically at least once every six months. Continuous monitoring of business relationships is performed with a frequency of no less than once every six months.

29. Detailed demonstrative list of signs of suspicious trade

Optional features of suspicious transactions

A business is considered suspicious if, for example:

- the client acts as if he were acting for or for someone else, is accompanied or monitored by another person or persons who appear to want to remain anonymous;
- the client performs activities that may help to obscure his or her identity or obscure the identity of the beneficial owner;
- the client or beneficial owner is a person from a country at risk;
- the liable person has doubts about the veracity or completeness of the data obtained about the client. The context shows, for example, that the client tries to provide inaccurate or incomplete information about himself;
- identification documents have a dubious appearance;
- the client is nervous, refuses identification or is reluctant to do so, or provides false information for his identification or control (eg the origin of money or the field of business);
- the client's criminal history or contacts or ties to persons connected with criminal groups or directly committing crime are known;
- the client has contacts or ties with risky countries;
- the client requests transactions that are unusual or performed in an unusual way, he rushes to complete the transaction more than is usual for similar transactions;

- the client makes transfers of assets that clearly have no economic reason, or carries out complex or unusually large transactions;
- during one day or in the days immediately following the client carries out noticeably more monetary operations than is usual for his activity or the activity of a comparable type of client;
- the funds handled by the client clearly do not correspond to the nature or scope of his business or his assets;
- the client operates in a field associated with the risk of connection to criminal groups (eg erotic services, discos and other nightclubs, trade in military equipment and especially weapons, etc.);
- the client knowingly carries out loss-making transactions or transactions with a disproportionate amount of the contractual penalty;
- transactions are carried out with a large amount of currency of lower value, or with an unusual transfer of a higher volume of cash (eg plastic bags, pockets of clothing, etc.);
- transactions are directed to or from areas where the client usually does not have or cannot be expected to have business interests;
- transactions are carried out in an amount just below the threshold of mandatory identification or control of the client.

Mandatory signs of suspicious transactions

- In the situations listed below, the trade is always suspicious and it is therefore reasonable to report the suspicious trade
- the client or the real owner is a person against whom the Canada applies international sanctions pursuant to the sanctions legislation;
- the subject of the trade is or is to be goods or services against which the Canada applies sanctions pursuant to the sanctions legislation;
- the client refuses to submit to the inspection or refuses to provide the identification data of the person for whom he acts;
- and other red flags described in the FATF guidelines

30. Non-Acceptable Customers

1. The Company maintains a comprehensive list of prohibited risk. Customers who exhibit these risk factors do not align with the Company's risk appetite. In instances where such risk factors manifest during the customer's onboarding process, the Company will decline to establish a business relationship or execute transactions with such customers. If prohibited risk factors are identified during an established business relationship, the relationship shall be terminated in accordance with the provisions outlined in this Program.
2. The prohibited risk factors encompass not only those related to low, medium, and high-risk categories but also extend to include customers from sanctioned countries and those originating from countries on the Financial Action Task Force (FATF) blacklist.
3. The Company is strictly prohibited from opening anonymous accounts or accounts registered under clearly fictitious names. Additionally, the Company refrains from initiating any form of business relationship or account setup without requesting and verifying customer identity data. This stringent requirement is upheld to counteract potential instances of fraudulent or falsified data within these documents.
4. The Company maintains a resolute stance against maintaining correspondent relationships with shell banks. Shell banks are defined as financial institutions or entities engaging in financial activities akin to those of a financial institution. These entities are incorporated in jurisdictions where they lack a physical presence, substantial management and oversight, organizational structure, and internal control systems. Furthermore, shell banks operate independently and are not affiliated with a financial group subject to supervision by competent authorities. The Company's refusal to engage with shell banks reinforces its commitment to rigorous risk management practices and compliance with anti-money laundering (AML) regulations. This prohibition extends to all shell banks, irrespective of their geographic location or origin.

31. Rules and procedures governing the offering of the liable person's services or products to third parties acting in the name and on behalf of the liable person

A third party is the person or entity that instructs another person or entity to conduct a transaction or activity on their behalf. As such, the third party is the instructing party to the transaction or activity, and is also understood to be the "on behalf of" party.
Third parties acting on the basis of a power of attorney or authorization on behalf of the liable person MINTPAY LTD.., follow the instructions according to the ***PCMLTFR, SOR/2002-184, ss. 134(2), 135(2), 136(2), 137(2).***, the current version of which is available on the liable person's website.
These persons were duly informed by the liable person about the obligations arising from ***Proceeds of Crime (Money Laundering) and Terrorist Financing Act (S.C. 2000, c. 17)*** The contractual partners of the liable person (especially the regional representatives) were duly instructed and trained by the liable person on these obligations, which they confirmed with their signatures on the attendance list. Authorized employees of the gaming house were duly informed about these duties and trained by the contractual partners of the liable person, which they confirmed with their signatures on the appropriate form.
Upon the receipt of a sum exceeding $10,000 in cash or virtual currency, necessitating the submission of a Large Cash Transaction Report (LCTR) to FINTRAC or the maintenance of a record for significant cash transactions, it is imperative to employ reasonable measures to ascertain whether the individual providing the cash is representing a third party. (Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations (PCMLTFR), SOR/2002-184, s. 134(1).) It is essential to note that this obligation is contingent upon compliance with the 24-hour rule. (PCMLTFR, SOR/2002-184, s. 126.)

32. Continuous monitoring of trade relations, including trade review carried out during the relationship.

The obliged entity must obtain the information necessary to carry out ongoing monitoring of the business relationship (according to the other points listed here) and review the transactions carried out during the relationship to determine whether the transactions are consistent with what the obliged entity knows about the client and his business and risk profile. The liable entity must be able to assess whether the

individual transactions are actually related to, for example, the client's business or his usual income, whether they correspond to his normal activities, etc. The liable entity also uses local and personal knowledge of clients for these purposes.

The client is obliged to MINTPAY LTD.. provide the information necessary to carry out the identification, including the submission of relevant documents. The company may make copies or extracts from the submitted documents and process the information thus obtained to fulfill the obligations under the AML Act.

If the identity card on the basis of which the identification is performed does not state the address of permanent or other residence, place of birth or information on citizenship, the person subject to identification is always obliged to prove these identification data to the bank in an alternative manner. Evidence of this information may be provided either by submitting another document that proves the missing identification data and is accepted by the Bank, or in the form of its written affidavit. A person is only identified if all his / her identification data required by law, ie including those not mentioned in the identity card, are ascertained, verified and recorded and must be ascertained in another way, for example on the basis of his / her solemn declaration.

32.1.Additional information for client identification and monitoring

The client shall provide the liable person with the information necessary to carry out the identification. The client also assumes active cooperation from the client, which may consist, for example, in the submission of relevant documents and declarations. The client must be informed that the information obtained is required on the basis of the AML Act (the duty of confidentiality applies only to the possible submission of an STR and an investigation by the FINTRAC).

The liable person may make copies or extracts from the submitted documents and process the information obtained to fulfill the purpose of the AML Act. However, making copies is conditional on obtaining the client's consent.

In other transactions with an already identified person (or during the duration of the business relationship), the liable person shall verify the identity of the specific natural person acting in an appropriate manner.

Furthermore, the liable person checks the validity and completeness of the client's identification data, information obtained during the client's inspection, the justification for the simplified client's inspection or exceptions from the client's inspection and records their changes.

All data are recorded in the questionnaire "Record of meetings" of MINTPAY LTD.., which is filled in in accordance with the requirements of the PCMLTFA and AML.

33. Transaction Records

MINTPAY LTD.. maintains electronic records of all transactions processed through our systems, regardless of type, status, or amount.

All transaction records are retained for a minimum of 5 years in accordance with FINTRAC guidelines, and will be stored for the duration of MINTPAY LTD..'s business operations unless a client specifically requests the deletion of their information in accordance with the terms governing privacy and consent in their jurisdiction.

- When performing individual transactions, when establishing a business relationship with a client, as well as during the obligated person:

• provides and stores such information about the client that will enable it toevaluate whether it is a risky client;

• checks the validity and completeness of client data and updates them;

• pays increased attention to shops;

• for which any of the risk factors determined on the basis of the performed ML / FT risk assessment occur;

• performed with natural persons as part of services based on an individual approach to the client;

• with PEP;

• for which the obligated person is aware that the real owner of the client is PEPor that PEP will participate in them otherwise;

• large volume or high level of complexity, especially with regard to the type of client, the subject, amount and method of settlement of the transaction, the

purpose of the business relationship and the subject of the client's activity.

34. Ongoing monitoring

The obligation to control the client does not need to be fulfilled in the following situations:

For financial entities: Continuous surveillance is not required for group plan accounts within a dividend or distribution reinvestment plan (including plans enabling members to acquire additional shares or units with contributions other than those from plan sponsors), provided that the plan sponsor: (PCMLTFR, SOR/2002-184, s. 146(2)(a).)

- Is a corporate entity with shares or units traded on a Canadian stock exchange.
- Operates within a country that is a member of the Financial Action Task Force (FATF).
- For insurance companies, brokers, or agents: Ongoing monitoring is not obligatory when engaging in reinsurance activities. (PCMLTFR, SOR/2002-184, s. 146(2)(b)).

1.Ongoing monitoring on a risk basis means the scrutiny of transactions to identifying changes to the customer profile (for example, their behaviour, use of products and the amount of transactions), and keeping it up to date, which may require the application of enhanced measures. Monitoring transactions is an essential component in identifying transactions that are potentially suspicious. Transactions that do not fit the behaviour expected from a customer profile, or that deviate from the usual pattern of transactions, may be potentially suspicious.

2.MINTPAY LTD.. conducts regular reviews of transactions, at least on a weekly basis, to identify transactions that may pose a risk of money laundering or terrorist financing based on location or amount.

3.Enhanced due diligence is performed on clients who engage in high-volume daily transactions through internal reporting and operational procedures.

4.The Risk team at MINTPAY LTD.. conducts weekly reviews of high-volume or high-velocity transfers initiated by customers.

5.Continuous monitoring for sanctions, Politically Exposed Persons (PEP), and adverse media is carried out by SUMSUB, with daily alert checks conducted by

35. Application of international sanctions

With regard to the application of international sanctions, the Company maintains a system of measures aimed at supporting actions to maintain or restore international peace and security, protect fundamental human rights, and facilitate efforts to combat terrorism. The employee who draws up the contract with the client always checks the client's name with the lists of persons who are subject to international sanctions in the Canada, EU and US. If an employee of the Company becomes aware of reliable information that the client controls assets subject to international sanctions, the employee must notify the AML authorized person, who will then notify FINTRAC without undue delay. The notification must be made by the Company in writing or orally in the form of a protocol or, in case of urgency, electronically or by fax.

In accordance with the Special Economic Measures Act (S.C. 1992, c. 17) and the Justice for Victims of Corrupt Foreign Officials Act (Sergei Magnitsky Law), S.C. 2017, c. 21, MINTPAY LTD.. ensures transactions and clients are screened against sanctions lists. Any identified matches will be reported to FINTRAC as part of the Suspicious Transaction Reports (STR).

MINTPAY LTD.. commits to adhering to the reporting requirements for **sanctioned property** as per the amendments to the Proceeds of Crime (Money Laundering) and Terrorist Financing Suspicious Transaction Reporting Regulations (SOR/2007-121), effective July 5, 2024, issued by the Canadian Department of Finance.

Identify transactions involving individuals or entities listed under sanction regimes, including Special Economic Measures Act (S.C. 1992, c. 17), Justice for Victims of Corrupt Foreign Officials Act (Sergei Magnitsky Law), and United Nations Act (R.S.C., 1985, c. U-2). Submit reports to the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) regarding identified sanctioned assets as soon as practicable (according to FINTRAC's requirements, the completion and submission of an STR should be treated as a top priority over other responsibilities).

Implement internal monitoring systems to analyze all incoming and outgoing

payments for compliance with international sanctions.

35.1.Sanctions Policies

In addition to AML/CTF framework, this Program also covers the Company's obligations related to the implementation of sanctions legally binding to the Company. The Company follows the Order on Sanctions, issued by FINTRAC and takes measures to ensure compliance with the relevant regulations and legislation on sanctions in Canada. It is particularly vital that the Company is able to identify sanction subjects and transactions violating sanctions, which may arise in the course of the Company's business activity. The Company takes into account at least the following sanction regimes:

• Consolidated Canadian Autonomous Sanctions List;
• United Nations Security Council Sanctions;
• European Union Sanctions;
• Office of Foreign Assets Control Sanctions.

By the decision of the AML Officer, the Company may follow other sanction regimes and restrictive measures.

1 Definition: Sanctions encompass a set of measures or actions taken to exert influence on the behavior, policies, or actions of a target entity. These sanctions consist of three key components:

• An economic action.
• Imposed on a target, which can be a state, a class of individuals, a specific person, or a function.
• With the intent of influencing the actions of the target.

2 Types and Implementation of Sanctions

Sanctions may encompass a variety of actions aimed at limiting trade, financial transactions, diplomatic relations, and the mobility of entities. They can be broadly categorized as specific or general measures, and their enforcement varies accordingly. Sanctions are commonly referred to as restrictive measures.

3 Sanctions Compliance involves the act of adhering to legislative, regulatory, and normative requirements related to sanctions.

- Objectives of Sanctions:

Sanctions serve multiple purposes within the international community, including:

• Encouraging a change in the behavior of a targeted entity or government.
• Preventing and suppressing the financing of terrorism and terrorist acts.
• Applying pressure on a target country to achieve specific objectives.
• Providing an enforcement tool when diplomatic efforts have proven ineffective.

- Functions of Sanctions

Sanctions serve as an extension of a nation's foreign policy, aiming to induce behavioral changes in other nations. They can be utilized for purposes such as deterrence, prevention, and punishment.

- Types of Sanctions

Sanctions may be applied geographically or thematically:

• Geographic Sanctions: Target specific countries or regions, exemplified by sanctions against North Korea or Crimea.
• Thematic Sanctions: Focus on issues or concerns that transcend geographical boundaries, as seen in counternarcotics sanctions.

4 Beyond Safeguarding Human Rights and averting military conflict, sanctions have been employed for:

• Preventing armed conflicts.
• Promoting democratic values.
• Punishing human rights violators.
• Preventing nuclear proliferation and the spread of weapons of mass destruction.
• Securing the release of detained citizens.
• Restoring sovereignty over disputed territories.

35.2.Sanctions Laws

1.Compliance with Canadian Sanctions Laws:

MINTPAY LTD.., a licensed Money Service Business (MSB) operating in Canada, is committed to upholding Canadian sanctions laws.

2.Canadian sanctions laws:

• Prohibit individuals and businesses from engaging with designated individuals, jurisdictions, and specific sectors.
• Impose screening, reporting, and asset-freeze obligations on regulated financial

institutions and other prescribed entities.

3.Federal Statutes for Economic Sanctions

The Government of Canada enforces economic sanctions under three federal statutes:

• The Criminal Code.

• United Nations Act.

• Justice for Victims of Corrupt Foreign Officials Act.

4.Additional Acts Related to Trade Restrictions and Related Measures Include:

• Special Economic Measures Act.

• Freezing Assets of Corrupt Foreign Officials Act.

- Adherence to Multiple Sanctions Laws:

5.In addition to Canadian sanctions laws, the Company is committed to adhering to other international sanctions regimes. **Annex No. 2**

- These international sanctions regimes include but are not limited to:

• United Nations Security Council Sanctions.

• European Union Sanctions.

• Office of Foreign Assets Control Sanctions.

6 Compliance with Sanctions Laws:

- Compliance with sanctions laws is a fundamental aspect of the Company's risk management and regulatory compliance efforts.
- Failure to comply with sanctions laws can lead to severe legal and reputational consequences, including fines, penalties, and damage to the Company's business relationships.
- Designated Individuals and Entities:
- The Company is committed to identifying and screening designated individuals, jurisdictions, and entities subject to sanctions.
- The screening process includes checking against the following lists, among others:

• Consolidated Canadian Autonomous Sanctions List.

• United Nations Security Council Sanctions List.

• European Union Sanctions List.

• Office of Foreign Assets Control Sanctions List.

7 Transaction Monitoring:

- The Company employs robust transaction monitoring mechanisms to identify and

prevent transactions that may violate sanctions laws.

- Suspicious or potentially sanctioned transactions are subject to further investigation and potential reporting to relevant authorities.

8 Reporting Obligations:

- The Company is obligated to report any identified sanctions violations to the appropriate regulatory authorities.
- Reporting is a crucial aspect of maintaining compliance with sanctions laws and cooperating with law enforcement agencies.

10 Training and Awareness:

- All employees of the Company are required to undergo training and awareness programs to understand and adhere to sanctions laws and regulations.
- Ongoing training ensures that employees remain vigilant and capable of identifying potential sanctions violations.

11 Review and Update:

- The Company's sanctions policies and procedures are subject to regular review and update to ensure alignment with evolving sanctions laws and regulations.
- Any changes in sanctions laws or international sanctions regimes are promptly incorporated into the Company's policies.
- Record Keeping:
- The Company maintains detailed records of all sanction-related activities, including screening results, investigations, and reports.
- Accurate record-keeping is essential for audits and demonstrating compliance with sanctions laws.

Currently, sunctioned countries are:
Afghanistan, American Samoa, Angola, Bahamas, Belarus, Botswana, Burundi, Cambodia, Central African Republic, Chad, Congo, Cuba, Democratic Republic of Congo, Equatorial Guinea, Eritrea, Ethiopia, Ghana, Guam, Guinea Bissau, Iran, Iraq, North Korea, Lebanon, Libya, Mali, Nigeria, Pakistan, Panama, Puerto Rico, Samoa, Saudi Arabia, Sierra Leone, Somalia, South Sudan, Sri Lanka, Sudan, Syria, Trinidad and Tobago, Tunisia, Venezuela, Yemen, Zimbabwe, Belarus, Russian Federation.

35.3.International sanctions against Russia

Since 2014, the EU has progressively imposed sanctions on Russia in response to the

crisis in Ukraine. Following the Russian invasion into Ukraine in February 2022 and the ongoing military aggression, more comprehensive and robust sanctions have been imposed by the EU in six sanctions packages against Russia on 23 February, 25 February, 28 February/2 March, 15 March, 8 April and 3 June 2022.

The measures include:

- individual sanctions (asset freezes, prohibition to provide funds or economic resources)
- economic sanctions (restrictions on exports and imports and the provision of services)
- media sanctions.

The basic legal acts are Council Regulation (EU) No. 269/2014 (regarding individual sanctions) and Council Regulation (EU) No. 833/2014 (all other sanctions), as amended by each sanctions package.

Financial services/business services

In the financial services/business service sectors, the EU imposed restrictive measures regarding the provision of financial services and access to EU capital markets, as well as bans on providing SWIFT services to certain banks and restrictions on providing rating services and certain accounting and consulting services.

Prohibition to purchase, sell or deal with securities issued by certain Russian banks, the Russian Central banks and certain entities, or to provide investment services for or assistance in the issuance of these securities.

Prohibition to make or be part of any arrangement to make new loans to certain Russian banks, the Russian Central banks and certain entities.

Prohibition to provide public financing or financial assistance for trade with, or investment in, Russia.

Prohibition to invest, participate or otherwise contribute to projects co- financed by the Russian Direct Investment Fund.

Prohibition to sell, supply, transfer or export banknotes denominated in any official currency of a Member State to Russia or for use in Russia. Prohibition to accept deposits from Russian persons/persons residing in Russia, if total value of deposits exceeds CAD 100,000.

Prohibition to provide rating services to any Russian national or natural person residing in Russia or any legal person, entity or body established in Russia.

Prohibition to provide certain consultancy services such as accounting, auditing (including statutory audit), bookkeeping and tax consulting services, business and management consulting, and public relations services to the Russian government, as well as to legal persons, entities or bodies established in Russia.

Prohibition to act as, or arrange for another person to act as, a trustee, nominee shareholder, director, secretary or a similar position, for a trust or similar legal arrangement, where the trustor or beneficiary is Russian. SWIFT ban for the following banks:

- Bank Rossiya
- Credit Bank of Moscow • Novikombank
- Otkritie FC Bank
- Promsvyazbank
- Rosselkhozbank JSC
- SberBank
- Sovcombamk
- VEB/Vnesheconombank • VTB Bank.

Restriction of trade with the regions of Crimea, Sevastopol, Donetsk and Luhansk

The EU also has imposed restrictions on dealing with the non- government controlled areas of Crimea, Sevastopol, Donetsk and Luhansk by Council Regulation (EU) No. 2022/263. The restrictions are much like the restrictions the EU has imposed on Crimea and Sevastopol since 2014 in Council Regulation (EU) No. 692/2014:

The EU has imposed a general import ban on any goods originating in the regions of Crimea, Sevastopol, Donetsk and Luhansk. Financing or financial support, insurance or reinsurance relating to the import of such goods is equally prohibited.

The EU has imposed an export ban of certain listed goods from the transport, telecommunications and energy sectors, or the prospecting, exploration and production of oil, gas and mineral resources in the regions of Crimea, Sevastopol, Donetsk and Luhansk. Technical assistance, brokering or financing or financial assistance regarding these goods are equally prohibited.

The EU has imposed certain investment prohibitions, e.g. regarding the acquisition of real estate, (shares of) companies or regarding the creation of joint ventures in the regions of Crimea, Sevastopol, Donetsk and Luhansk.

The EU has imposed a prohibition to provide services directly related to tourism activities in the regions of Crimea, Sevastopol, Donetsk and Luhansk.

Exemptions are available under certain circumstances.

Restrictions of trade with Belarus

In response to the involvement of Belarus in the Russian invasion into Ukraine the EU has also substantially widened the economic sanctions imposed on Belarus by Council Regulation (EU) No. 765/2006. The sanctions include:

individual sanctions against 195 individuals and 35 entities (asset freeze, prohibition to provide funds or economic resources, travel ban) economic sanctions (restrictions on exports and imports and the provision of services)

a SWIFT ban for five Belarusian banks

a prohibition on transactions with the Central Bank of Belarus

limits on the financial inflows from Belarus to the EU

a prohibition on the provision of euro-denominated banknotes to Belarus.

36. Reporting

A suspicious transaction report (STR) is a type of report that must be submitted to FINTRAC by an RE if there are reasonable grounds to suspect that a financial transaction that occurs or is attempted in the course of their activities is related to the commission or the attempted commission of an ML/TF offence (Proceeds of Crime (Money Laundering) and Terrorist Financing Act, S.C. 2000, c. 17, ss. 7(a) and 7(b).). Procedure from the detection of suspicious trade to the moment of delivery of the FINTRAC notification, rules for processing suspicious trade and identification of persons who evaluate suspicious trade.

SITUATION WHEN STR IS SUBMITTED TO THE FINTRAC

The liable person shall report the suspicious transaction on the basis of the above, but in particular if:

- doubts remain about possible misuse of ML / FT even after the client's inspection;
- the client refuses to identify before the trade and the liable person has partial information about the client or (in these cases all information from the liable person's representatives concerning the description, behaviour, course of negotiations with an unidentified trade participant, his arrival and departure is included in the STR; the basic identification data of the employees of the liable person who dealt with the unidentified participant in the trade and could, if necessary, further supplement its description or carry out its subsequent identification) are given;
- the client does not cooperate in obtaining data and information in the identification and control of the client (in this case the liable entity will consider according to the current situation whether the presumption of obtaining an appropriate explanation from the client is postponement of cooperation and submission of STR until its expiration);
- the liable person is not aware of the origin of the property used in the PEP trade from public sources and this person refuses to explain the origin of the property;
- are compulsory reasons pursuant to subsection 9(2) of the Proceeds of Crime (Money Laundering) and Terrorist Financing Suspicious Transaction Reporting Regulations
- this is not a specific suspicious trade, but "other facts" that could indicate money laundering and terrorist-related trafficking.

If the liable person discovers a suspicious transaction in connection with its activities, and has reasonable grounds to suspect (RGS) that a transaction is related to the commission of an ML/TF offence, it shall notify the FINTRAC as soon as practicable (Proceeds of Crime (Money Laundering) and Terrorist Financing Suspicious Transaction Reporting Regulations (PCMLTFSTRR), SOR/2001-317, s. 9(2).

As soon as practicable is interpreted to mean that the liable person has completed the measures that have allowed them to determine that they reached the RGS threshold. As such, the development and submission of that STR must be treated as a priority.

If the circumstances of the suspicious case so require, in particular if there is a risk of delay, the liable person shall notify the suspicious transaction immediately

after its discovery. This procedure is necessary in a situation where there is a risk that the property that is the subject of trade, respectively. the means used in the transaction could escape the reach of law enforcement authorities by complying with the client's order. In this case, the liable person must report the suspicious transaction immediately after its discovery, even at the cost that the notification will not contain all relevant information (the notification will be supplemented subsequently).

There is no monetary threshold associated with the reporting of a suspicious transaction. Under the Canadian anti-money laundering and anti-terrorist financing (AML/ATF) regime, STRs may contain transactions that must be submitted to FINTRAC in other types of reports. For example, if a completed transaction reported in an STR involved the receipt of cash from a client of 10,000 Canadian Dollars (CAD) or more, the liable person would also be required to report this transaction to FINTRAC in a large cash transaction report (LCTR).

Notifications and Reporting to the Bank of Canada:

1. Notification of significant changes:

The company must notify the Bank of Canada about significant changes, including:

- Introduction of new services or technologies.
- Changes in business processes affecting risk management.
- Participation in new partnerships.

2. Incident reporting:

In the event of incidents, such as data breaches or system failures, the company must submit a report to the Bank of Canada within 10 business days.

The report should include:

- A description of the incident.
- Measures taken to respond.
- A plan to prevent recurrence.

3. Annual reporting:

The company is committed to providing an annual report to the Bank of Canada that includes:

- An overview of operational risk management.

- A list of implemented improvements.
- Details about customer fund protection measures.

36.1. The procedures for submitting a Suspicious Transaction Report (STR) to FINTRAC

Electronic reporting:

In accordance with subsection 9(2) of the "Proceeds of Crime (Money Laundering) and Terrorist Financing Suspicious Transaction Reporting Regulations," suspicious transaction reports (STRs) are submitted through FINTRAC's Web Reporting. To do this, the liable person will utilize FINTRAC's secure website. In the event that submission through Web Reporting is not possible or convenient, the liable person can opt for an alternative method, such as batch file transmission.

Paper reporting:

The liable person can obtain a paper Suspicious Transaction Report (STR) form on the FINTRAC reporting forms webpage. Alternatively, the liable person can request the paper form to be sent by fax or mail by contacting FINTRAC at 1-866-346-8722. To ensure the clarity and legibility of the provided information and to facilitate the data entry process, the liable person should fill in the text sections of the STR (parts G and H) using a text editor. If reports are filled out by hand, black ink and CAPITAL LETTERS should be used.

The completed paper STR form can be submitted to FINTRAC through two methods:
By fax: Fax number: 1-866-226-2346.
By mail to the following address:
Financial Transactions and Reports Analysis Centre of Canada
Section A
234 Laurier Avenue West, 24th floor
Ottawa, ON K1P 1H7
CANADA

36.2. Opportunities STR

STR contains all information available to the notifier about this trade, its context and its participants, namely:

1. Identification of the notifier of the suspicious transaction:

business name (name and surname or name including distinguishing appendix) or other designation, registered office (or address for delivery), identification number, subject of business according to the entry from the Commercial Register or (only the subject of business related to the notification shall be stated) and the type of liable person with reference to the relevant provision of the AML Act (indicate the relevant paragraph, letter and point corresponding to the type of liable person);

2. The identity of the person to whom the notification relates, as follows:

- **natural non-business person:** name and surname, including any other names and surnames used (in case of dispute, clearly distinguish name and surname), address of residence in the Canada or outside the Canada and other addresses used, birth number or date of birth, place of birth, the type and number of the identity card, when and by whom it was issued and information on its validity, nationality, sex (if not clear from other information), or other identification data stated in the identity card;
- **natural entrepreneurial person:** in addition to data for a natural non-entrepreneurial person, supplements used in business, or business company registered in the Commercial Register and identification number, subject of business according to the trade license or according to the entry in the Commercial Register and place of business;
- **legal entity:** business name or name, including a distinctive supplement or other designation, registered office, identification number or similar number assigned abroad, name, surname, birth number or date of birth and residence of persons who are its statutory body or its member, if statutory body or its member, a legal entity, then its business name or name, including a distinctive supplement or other designation, place of business, identification number and identification data of persons who are its statutory body or its member, identification data of themajority shareholder or controlling entity.

In the case of representation of a natural person and always in the case of a legal person, the identification details of the person acting on behalf of the person to

whom the notification relates;

3. The identification details of all other participants in the trade which are available to the obliged entity at the time of notification.
4. A detailed description of the subject matter and material circumstances of the suspicious transaction, in particular:

• the reason for the transaction given by the trader;
• a description of the cash or other means of payment used and other circumstances of the cash payment;
• time data;
• the numbers of the accounts on which the funds in respect of which the notification is made are concentrated and the numbers of all accounts to or from which the money has been or is to be transferred, including the identification of their owners and disposers, if this information is accessible;
• menu;
• what suspects the business;data on related transactions
• a description of the behavior of the trade participant and its potential partners;
• where appropriate, the identified telephone and fax numbers, description and registration numbers of the means of transport;
• other information that could be of informational importance to the persons involved or the transaction in question, as well as other data that may be related to the suspicious transaction and are relevant for its assessment in terms of AML / CFT prevention (Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations (PCMLTFR), SOR/2002-184, s. 85(1).);

the notification shall include:

- copiesof all documents mentioned in this notification and related to the subject of the notification;
- financial instruments or mechanisms that were used to conduct the transaction;
- transaction place;
- ML/TF indicators used to support your suspicion;
- suspected criminal offence related to ML/TF
- description «how did the transaction take place»

5. A warning in the event that the notification also concerns property subject to

international sanctions declared for the purpose of maintaining or restoring international peace and security, protecting human rights or combating terrorism. Along with the notification, a brief description of the property, details of its location and its owner, if known to the notifier, shall be provided. In addition, information shall be provided on whether there is an imminent risk of damage, deterioration or use of such property in contravention of the law;

6. The notifier shall always state whether and when the trade was executed or whether it was postponed, or the reason why the trade was or was not executed.

Contact information:

- The STR must contain the name, surname and job classification of the person submitting this notification on behalf of the liable person and the possibility of contact to receive instructions from the FINTRAC, including the possibility of contact outside normal working hours (telephone, fax, e-mail);
- furthermore, the STR contains the date, time and place of submission of the notification and the signature of the person fulfilling the notification obligation;
- the STR does not provide data on the employee of the liable person or a person in a similar employment relationship who has discovered a suspicious transaction.
- The liable person may not inform the client about the submission of the STR.

Exclusions:

The suspicious transaction reporting requirement does not apply to the operations of foreign subsidiaries or foreign branches or branches outside Canada.

36.3. Reporting suspicious activities of staff members to an authorized liable person

The Company is bound by statutory and regulatory obligations that mandate the disclosure of information to the Anti-Money Laundering (AML) Officer under specific circumstances. These circumstances encompass situations in which:

- An employee possesses actual knowledge or suspicion of money laundering or terrorist financing.
- An employee has reasonable grounds to know or suspect that another person is

involved in money laundering or terrorist financing.

Company employees are required to make disclosures not only when they have definite knowledge or suspicion of money laundering or terrorist financing but also when, given the circumstances, such knowledge or suspicion should reasonably have been reached, and yet it was not. Any knowledge or suspicion must be reported promptly to the liable person as outlined below. Employees must avoid any unjustifiable delays in making such disclosures.

In the event that the need to notify the liable person arises, this notification process shall involve the completion of an internal report using the approved form. The internal report should be prepared and signed by the liable person. The signed internal report must be sent to the AML Officer's email as expeditiously as possible, with a maximum delay of 24 hours from the time the obligation to report arises.

37. Confidentiality provisions

The purpose of the duty of confidentiality under Privacy Act and the Charter of Rights and Freedoms is in particular:

- uninterrupted investigation of suspicious trade;
- protection of processed and stored information until the results of the investigation are passed on to another authority;
- maintaining the possibility of applying precautionary measures against property in possible subsequent criminal proceedings;
- protection of whistleblowers from threats or hostile acts. The duty of confidentiality applies to: the filing of an STR and its investigation; securing property;
- Personal information shall be received, collected, used, disclosed and disposed of in compliance with the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA), the Privacy Act, and the Library and Archives of Canada Act;
- Everyone who learns about the facts that are subject to confidentiality is obliged to maintain confidentiality;

In carrying out its mandate under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA), V A L L I S P A Y M E N T S L T D. receives and collects personal information about individuals as defined by section 3 of the Privacy Act.

Personal information must be safeguarded at a proportionate level in relation to relevant statements of sensitivity and threat risk assessments in order to ensure that personal information is not at risk of being misused or mishandled. Also, personal information must be protected from improper access, loss, use, disclosure or destruction through the inclusion of specific confidentiality provisions in contracts or other arrangements with third parties.

Access to personal information shall be limited to those who have a need-to-know in order to effectively perform their duties and functions.

38. Program

MINTPAY LTD. has established and continuously maintains an ongoing Anti-Money Laundering and Counter-Terrorist Financing (AML-CTF) training program to ensure that all staff members possess a comprehensive understanding of the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA) and their obligations under this legislation (PCMLTFR, SOR/2002-184, s. 156(1)(d).).

The training program cover:

Technical aspects of monitoring virtual asset transactions in compliance with **MiCA.**

Protocols for filing suspicious transaction reports with FINTRAC.

Advanced approaches to monitoring PEP accounts and cross-border operations.

Expanded Text of Additions to the AML Policy in Compliance with Bank of Canada Requirements (Excluding the Insurance Clause)

1 Minimum Training Requirements:

- All staff members are obligated to complete this training within the first two weeks of their employment.
- Subsequently, team training sessions are conducted at least once annually.

2 Training Content:

- The training program is delivered internally and comprises dedicated content provided by the company's in-house AML specialist as well as external providers.
- Seminars and Training Sessions: These are conducted both internally within the

company and externally through training organizations. They cover a wide range of topics, encompassing general AML/CTF principles and industry-specific requirements and practices.

- Employees are mandated to digitally confirm that they have been provided with, read, and comprehended all AML training documentation.
- Compliance staff members are required to possess appropriate certification and relevant experience, in addition to maintaining their Continuing Professional Education (CPE) requirements for certification.

3 Supplementary Training and Awareness:

- The liable person may periodically develop and disseminate supplementary training materials and awareness resources on an ad hoc basis.
- Compliance staff members are mandated to be included in the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) mailing list and consistently review all correspondence originating from FINTRAC.

Program Structure:

The following categorization and training level system has been developed with the aim of optimizing compliance training with AML/CFT requirements and encompasses the following provisions:

Category 1: AML Department Staff

Employees in the AML department have the highest priority in the training system, as they are responsible for developing, implementing, and overseeing the entire AML/CFT compliance program.

Training: This category receives the most comprehensive and in-depth AML compliance training, including the opportunity for external training at seminars and conferences to learn about advanced practices and changes in AML legislation.

Training Methods:

- Online training: workshops, seminars, certification courses
- Offline training: workshops, seminars, certification courses

- Self-study
- Conferences

Training content includes:

- Laws and regulations governing AML/CFT
- Establishing and adhering to internal AML/CFT procedures and policies
- Methods for monitoring and detecting suspicious transactions
- Reporting and interaction with regulatory authorities
- Advanced aspects of AML/CFT compliance
- Updates in legislation and best practices
- Recommendations from FATF and other international organizations

Training providers include external organizations such as the Association of Certified Anti-Money Laundering Specialists (ACAMS) and the Canadian Anti-Money Laundering Institute (CAMLI).

Training Frequency: Once a year or as needed:

- Training for new employees
- Introduction of new AML regulations by the governments of Canada, the USA, and European Union countries
- Publication of new FATF recommendations in AML regulation

Category 2: Employees Handling Financial Transactions

Training for employees handling financial transactions is of high importance, as they may encounter suspicious transactions in their work.

Training: The training will be comprehensive and focus on monitoring and detecting suspicious transactions.

Training providers include both internal AML compliance specialists and external organizations such as "FINTRAC Compliant AML Training" from learnedly, "AML/ CTF Employee Training" from Financial Crime Academy, and the Canadian Anti-Money Laundering Institute (CAMLI).

Training Methods:

- Online training: workshops, seminars, informational sessions

- Offline training: workshops, seminars, informational sessions
- Self-study materials

Training content includes:

- Compliance with AML/CFT and KYC regulatory requirements and the company's internal anti-money laundering/counter-terrorist financing policies
- Client identification and verification, KYC systems
- Transaction monitoring and documentation methods
- Reporting on suspicious transactions
- Various forms of money laundering and terrorist financing associated with company products and services

Training Frequency: Once every six months or as needed

Category 3: Employees with Client Interaction
Significance: This category is important, but their role in AML compliance may be less direct.
Training: Training will be less in-depth but cover the basic aspects of AML compliance.
Training Methods:
- Online training: workshops, seminars, informational sessions
- Offline training: workshops, seminars, informational sessions
- Self-study materials
Training content includes:
- Basics of AML/CFT laws and regulations
- Company policies and procedures for AML/CFT compliance
- Role in identifying and reporting suspicious transactions
- Reporting on suspicious transactions
Training providers are internal AML compliance specialists.
Training Frequency: Once every six months or as needed

Category 4: Other Employees
Significance: This category has the least significance in the context of AML/CFT compliance.
Training: Training will focus on fundamental concepts and procedures.
Training Methods:
- Offline training: workshops, seminars, informational sessions
- Self-study materials
Training content includes:
- Basics of AML/CFT laws and regulations
- Responsibilities within their role for compliance
- Reporting on suspicious activities
Training Frequency: Once every year or as needed

Control:

At the end of the basic training programs, a test is provided. To pass the test successfully, employees must score 80% or higher. Employees are allowed to retake the test until they achieve a passing score. However, if an employee cannot pass the test after four retakes, their access to the company's systems and performance of regular job duties may be restricted.

*Each training will be documented in the form of internal reports by MINTPAY LTD.., including the training date, a list of participants who completed the training, and the topics covered.

39. Data Retention

The Company is obligated to retain specific data and documents concerning its clientele and financial transactions. These documents and data should be preserved in a manner that enables comprehensive and immediate response to requests from the AML Officer, inquiries from the FINTRAC or, as mandated by legislation, other regulatory authorities, investigative entities, or the judiciary.

The Company shall adhere to all regulations governing the safeguarding of personal data as stipulated by the applicable laws. The processing of personal data collected during Customer Due Diligence (CDD) procedures is permissible solely for the purpose of preventing money laundering and terrorist financing. Under no circumstances shall this data be further processed in a manner incompatible with the designated purpose, such as for marketing endeavors.

Maintenance of Registration Logbooks

The Company is required to maintain the following registration logbooks, meticulously documenting financial operations and transactions (hereinafter referred to as "logbooks"):

Logbook for virtual currency exchange transactions or transactions involving virtual currency, with a value equal to or exceeding CAD 10,000 or its equivalent in another currency or virtual currency, irrespective of whether the transaction occurs through one or more related transactions.

Logbook for reporting suspicious monetary operations and transactions.

Logbook of customers with whom transactions or business relationships were declined or terminated due to breaches of anti-money laundering and counter-terrorist financing protocols.

The aforementioned data, based on documents substantiating a monetary operation or transaction or other legally valid documents related to the execution of such activities, should be chronologically entered in the relevant logbook immediately, but no later than within three business days following the conclusion of a monetary operation or transaction.

The storage of logbook data shall be executed and retained electronically, within the Company's internal system, and is the Company's responsibility to ensure logbook upkeep. A comprehensive list of the information to be included in each logbook is provided in the logbook template file.

The data contained within the logbooks shall be retained using software that allows for the export of stored details to Microsoft Office Excel, Word, or equivalent open-source software, while preserving the integrity of the information.

The maintenance of the registration logbooks is to be carried out in accordance with the "Order on Logbooks."

39.1.Data to be Retained and Retention Terms

1.Data Retention for 5 Years After Business Relationship Termination:

- Copies of the customer's identity documents, including beneficial owner and beneficiary identity data, along with direct video streaming/direct video broadcasting recordings and other information acquired during the customer's identity verification process. This includes wallet and/or agreement documentation in either original document format or electronic form.
- Logbooks, which may be stored in either paper or electronic format.
- Information enabling the linking of the virtual currency wallet to the owner's identity.

2.Data Retention for 5 Years After Transaction Completion:

- Documents validating financial operations or transactions, along with data and other legally binding documents pertaining to the execution of Monetary Operations or transaction finalization.

3. Data Retention for 5 Years After Business Relationship Termination: correspondence with the Customer during the Business Relationship, whether documented in paper or electronic form.

4.Data Retention for 5 Years: Internal investigation records of suspicious transactions, maintained in paper or electronic format.

5.Additional Provisions:

- The specified retention periods may be extended for a maximum of two years, subject to reasoned instructions from a competent authority.
- Deletion of retained data will be carried out after the prescribed time period lapses, unless regulations governing the relevant domain establish an alternative procedure or an extension of the retention periods is mandated by a competent authority. The AML Officer is responsible for data deletion.

40. Provisions on the preparation of evaluation reports of the liable person

The liable person shall prepare a report evaluating the obligated person's activities in the field of AML / CFT prevention pursuant to (PCMLTFR, SOR/2002-184, s. 156(3)), ensures that the effectiveness assessment of the AML system commences no later than one year (12 months) from the commencement of the previous assessment. Furthermore, the previous assessment must be completed.

The liable person ensures that the effectiveness assessment of the AML system commences no later than one year (12 months) from the commencement of the previous assessment. Furthermore, the previous assessment must be completed.

In this evaluation report, the liable entity shall assess whether:

- the procedures and measures applied by the liable entity in the field of AML / CFT prevention are sufficiently effective;

Deficiencies have been identified in the area of AML / CFT prevention in the past period and what risks may arise for the liable person, including proposals to remedy the identified deficiencies.

If the liable person has a statutory body, this body shall discuss the evaluation report no later than 4 months after the end of the period for which it is prepared, and shall comment on the identified deficiencies and the proposals contained therein. If the liable person has a supervisory board, a board of directors or a control commission, this body shall also perform these tasks. In the case of a branch, organizational unit or establishment of an institution, these duties are performed by its manager.

The purpose of an effectiveness review is to determine whether compliance program has gaps or weaknesses that may prevent your business from effectively detecting and preventing ML/TF.

The effectiveness analysis will help you determine whether the company's business practices reflect what is stated in corporate documents and corporate policy and whether MINTPAY LTD. complies with the requirements of PCMLTFA and its associated regulations.

It will also assess the effectiveness of the risk assessment system in identifying and mitigating ML/TF risks.

MINTPAY LTD. documents the verification process by an internal liable person or an external auditor at its discretion depending on operational circumstances (PCMLTFR, SOR/2002-184, s. 156(3)).

MINTPAY LTD. has developed and documented a one-year effectiveness assessment plan for the AML compliance program (PCMLTFR, SOR/2002-184, s. 156(1)(f)). (Annex No. 1)

41. Bindingness and effectiveness

The obligated person constantly monitors the development and changes in the fight against ML / FT (ie laws, decrees, government regulations, etc.) and trends in the development of risks associated with this area. The relevant regulations are published by the FINTRAC on the websites https://fintrac-canafe.canada.ca/guidance-

directives/compliance-conformite/Guide4/4-eng#fn202113 and the Government of Canada at https://lois-laws.justice.gc.ca/eng/acts/P-24.501/page-4.html#h-398586.
The site is for information purposes only and the active activity of the liable person is assumed. In the event of changes in the regulations, or new regulations are in force, the liable person shall bring the content of this document in accordance with these regulations and also ensure the training of all persons affected by such changes. Similarly to newly detected risks, the liable entity shall take the necessary additional measures to mitigate them.

For the company MINTPAY LTD., Tyler Jade Egginton, CEO.

Annex No. 1

EFFECTIVENESS EVALUATION

Objectives and Goals of Effectiveness Evaluation

The aim of our one-year effectiveness evaluation of the compliance program was to assess and confirm that our organization successfully adheres to anti-money laundering and terrorism financing (AML/TF) policies, procedures, and requirements. We sought to ensure that our actions are directed towards effectively complying with legislative norms and best practices in this field.

Elements of the Compliance Program:

- Policies and Procedures:
- Examination of our policies and corresponding procedures, including their content, clarity, and relevance.
- Analysis of policy integration into the company's operational processes and procedures, and how it is applied in practice.
- Evaluation of policy implementation by employees, including assessing their knowledge and adherence to the policy.

Evaluation Methods:

- Employee Interviews:
  - Assessment of knowledge among employees involved in financial operations regarding AML/TF policies and procedures.
- Records and Documentation Review:
  - Analysis of a sample of records and documentation related to financial transactions to determine how accurately and completely they adhere to our policies and procedures.
- Review of Agreements with Agents and Trusted Persons:
  - Examination of agreements with agents and trusted persons, and analysis of a sample of information they referred to during customer identity verification.
- Transaction Review:
  - Analysis of a sample of financial transactions to determine whether information on suspicious transactions was reported to relevant

authorities, such as FINTRAC, accurately and promptly.

- Large Cash Transaction Review:
    - Analysis of large cash transactions to assess whether reports to FINTRAC contained accurate information and were submitted within established deadlines. The sample size constituted 8% of the total number of large transactions.
- Electronic Fund Transfers Review:
    - Analysis of electronic fund transfers to determine if reported transfers to FINTRAC contained accurate information and were submitted within established deadlines, especially for renewable energy sectors with EFT obligations.
- Client Records Review:
    - Verification of client records to determine whether risk assessments were applied in accordance with our risk assessment process.
- High-Risk Client Records Review:
    - Inspection of a sample of records for high-risk clients to ensure that enhanced risk mitigation measures were adopted, including their existence and conformity.
- Documentation Review:
    - Examination of records and documentation to ensure compliance with proper procedures and requirements. Evaluation criteria included the accuracy and completeness of documentation.
- Risk Assessment Review:
    - Verification of the risk assessment to ensure that it reflects our current activities. Evaluation criteria included the accuracy and timeliness of the risk assessment.
- Review of Policies and Procedures:
    - Update (if necessary) and review of our policies and procedures to ensure they align with current legislative requirements and our current business practices. Evaluation criteria included the relevance and correctness of policies and procedures.

Scope of the Evaluation:

Policies and Procedures:

- Compliance of policies with legislative requirements.
- Clarity and comprehensibility of wording in policies.
- Relevance and updating of policies.

Policy Integration:

- Assessment of successful integration of policies into the company's operational processes and procedures.

Policy Implementation:

- Verification of the degree of policy implementation by employees, including an assessment of their knowledge and adherence to the policy.

Review of Agreements with Agents and Trusted Persons:

- Inspection of agreements and analysis of referenced information during customer identity verification.

Transaction Review:

- Analysis of large cash transactions to assess the accuracy and timeliness of reporting to FINTRAC.

Electronic Fund Transfers Review:

- Analysis of electronic fund transfers to assess the accuracy and timeliness of reporting to FINTRAC.

A responsible party will compile a detailed report on the progress and results of the evaluation.

*The performance review begins three months before the end of the one year period (12 months) from the start of the previous review.

Annex No. 2

LISTS OF SUSPECTED PERSONS AND RISK STATES

The annex contains links to lists of sanctioned persons and persons suspected of supporting terrorism and a list of countries at risk.

Canadian sanctions legislation

- https://www.international.gc.ca/world-monde/international_relations-relations_internationales/sanctions/legislation-lois.aspx?lang=eng
- Internetaddressof the FinancialAnalyticalOffice http://www.financnianalytickyurad.cz/
- Consolidated list of sanctioned entities https://eeas.europa.eu/headquarters/headquarters- homepage/8442/consolidated-list-of-sanctions_en
- List of risk states designated by the FATF (Financial Action Task Force on Money Laundering) http://www.fatf-gafi.org
- List of risk countries established directly by effective EU legislation https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02016R1675-20180306
- Sanctions list https://www.un.org/sc/suborg/en/sanctions/1267/aq_sanctions_list

Demonstrative list of sources of information on the level of corruption and other source of crime in foreign jurisdictions:

- Organization for Economic Co-operation and Development (corruption) http://www.oecd.org/corruption/
- Organization for Economic Co-operation and Development (tax havens) http://www.oecd.org/countries/monaco/list-of-unco-operative-tax-havens.htm
- Council of Europe - GRECO (corruption) https://www.coe.int/en/web/greco
- United Nations Office on Drugs and Crime (UNODC) http://www.unodc.org/

Annex No. 3

OVERVIEW OF POLITICALLY EXPOSED PERSONS OPERATING IN THE CANADA

A politically exposed person in the Canada is mainly:

I) The President, Prime Minister, Mayors, governors Senior officers of Judges of the Supreme, Members of the governing body, statutory officers of state-owned enterprises and companies controlled by the Canadian government.

- Leadership of political parties;
- Senior officers of the armed forces;
- Member of the canada's central bank
- Ambassador or Head of Diplomatic Mission;
- Statutory body of state enterprises and companies controlled by the state (https://www.osfi-bsif.gc.ca/Eng/fi-if/rtn-rlv/fr-rf/dti-id/Pages/GBE.aspx)
- Attorney General, Public Defender of Rights, Financial Arbiter;
- another natural person who is or has been in a significant public function with national or regional significance (Note: The assessment of whether it is in other cases a Politically Exposed Person will be carried out in cooperation with the person in charge of compliance)

II)

- A person close to the person mentioned in point I (a relative in the direct line, especially children, parents, grandparents), a sibling and a spouse or a registered partner; other persons in a family or similar relationship)

III)

- A person in a business relationship with a person referred to in point I) (partner or beneficial owner of the same legal entity, or trust fund or other legal arrangement without legal personality as the person referred to in point I);or is known to be in any other close business relationship with the person referred to in point I), or the beneficial owner of a legal person, or a trust or other legal arrangement without legal personality, which is known to have been created for the benefit of the person referred to in point (ad) (I).