COMPLIANCE POLICY

1. PURPOSE AND SCOPE

The international initiatives and regulations devoted to the maintenance at global scale of the struggle for the prevention of laundering of proceeds of crime and the financing of terrorism have accelerated in a considerable extent recently in line with the constantly increasing sensitivity of the international public opinion on the matter. As the case is with many other countries that share the same sensitivity; various legal regulations have been being enacted and a great importance is attached to the strengthening of the existing practices on the matter.

Payporter Ödeme Hizmetleri ve Elektronik Para A.Ş. (PayPorter) considers combating the laundering of proceeds of crime and financing of terrorism as a social responsibility that goes beyond compliance with the laws and regulations and attaches the highest importance to it. PayPorter also considers such combat as a key element of the harmony and integration with the international system.

The PayPorter Compliance Policy has been prepared in accordance with the provisions of the Law on the Prevention of Laundering of Criminal Proceeds (Law No. 5549), the Law on the Prevention of the Financing of Terrorism (Law No. 6415), the Law on the Prevention of the Financing of the Proliferation of Weapons of Mass Destruction (Law No. 7262), and the secondary legislation prepared within the framework of these laws. It also takes into account the National Risk Assessment prepared and published by the Financial Crimes Investigation Board (MASAK).

Mainstays of this policy are,

- The international initiatives, conventions and regulations, to which the Republic of Turkey is a party,
- Law, No. 6493 on Payment and Security Settlement Systems, Payment Services and Electronic Money Institutions, and the other applicable legislations in force, enacted on the basis of the said Law (regulations, communiques, etc.)
- Turkish Criminal Code (Articles 54, 55, 165 and 282),
- Turkish Criminal Procedure Law,
- The international standards and recommendations as well as the generally accepted approaches, methods and practices regarding the prevention of laundering of proceeds of crime and financing of terrorism,
- The Law on the Prevention of the Proceeds of Crime, and the other applicable legislations in force, enacted on the basis of the said Law, (regulations, communiques, etc.),
- Law, No. 6415 on the Prevention of the Financing of Terrorism, and the other applicable legislations in force, enacted on the basis of the said Law, (regulations, communiques, etc.),
- Law, No. 7262 on the Prevention of the Financing of Proliferation of Weapons of Mass Destruction, and the other applicable regulations in force, enacted on the basis of the said Law. (regulations, communiques, etc.)

The national and international legislation currently in force on the Prevention of Laundering Proceeds of Crime Law, the Prevention of the Financing of Proliferation of Weapons of Mass Destruction and the Prevention of the Financing of Terrorism, as well as the international standards and recommendations published on these issues and the generally accepted approach, In this policy document, prepared within the scope of the method and best practices, the main outlines of the application principles that our Company, company employees and business partners must comply with are presented below, and there are also complementary documents (procedure, workflow, etc.) containing detailed explanations prepared and specific to our Company regarding these issues are available.

In order for ensuring the compliance by PayPorter as required with the provisions of the "Law No. 5549 on the Prevention of Laundering of Proceeds of Crime", “Law No. 7262 on the Prevention of the Financing of Weapons of Mass Destruction”, “Law No. 6415 on the Prevention of the Financing of Terrorism” and the other regulations and secondary legislations on

the matter that have been issued on the basis of the said Act, and for the fulfilment by PayPorter of the provisions set forth within the said legislations, the following purposes are aimed within this document;

- Ensuring PayPorter's policies, procedures, and control methods are in compliance with the legal regulations mentioned above, the secondary regulations derived from them, and the regulations made by the institutions authorized by this legislation,
- Prevention of the use of the products and services of PayPorter for the purpose of the laundering of proceeds of crime, financing of terrorism and financing of proliferation of weapons of mass destruction,
- Assessment of the customers, transactions and services through a risk-based perspective for the purpose of the prevention of the risks of laundering of proceeds of crime, financing of terrorism and financing of proliferation of weapons of mass destruction,
- Conducting risk identification, assessment, monitoring, and mitigation of risks related to the violation, non-implementation, and evasion of asset-freezing decisions, and implementing advanced controls for the application of these sanctions.
- Provision of information to the staff members about the respective legal and administrative responsibilities thereof for the prevention of laundering of proceeds of crime, financing of terrorism and financing of proliferation of weapons of mass destruction,
- Identification of the in-house audit and training activities of PayPorter, and
- Protection of the national and international reputation and customer quality of PayPorter,

PayPorter's policy aimed at the prevention of the laundering of proceeds of crime, financing of terrorism and financing of proliferation of weapons of mass destruction is based on the international conventions and initiatives and the national legal provisions on the matter, and particularly on the company's considering such combat as a key element of the harmony and integration with the international system.

This policy articulates PayPorter’s dedication to combating money laundering, terrorist financing, and the proliferation and financing of weapons of mass destruction, in accordance with applicable international standards and regulatory requirements:

- Risk Management,
- Monitoring and Internal Control,
- Training.

This policy forms the general framework of a risk-based approach devoted to ensure the compliance of the Company with the obligations imposed by the applicable legislations in force regarding the prevention of the laundering of proceeds of crime and the prevention of financing of terrorism.

This policy covers PayPorter's Board of Directors, Senior Management, Head Office, domestic representative offices and branches, as well as branches, representative offices and subsidiaries abroad, unless otherwise stipulated in the legislation of the country in which they are located, and the managers and employees at all levels working therein, in terms of duties, authorities and responsibilities related to the prevention of laundering proceeds of crime and financing of terrorism and the prevention of the proliferation and financing of weapons of mass destruction.

2. RESPONSIBILITY

The responsibility for the enforcement of this policy as a whole, adequately and effectively, shall be fulfilled finally and conclusively by the Board of Management of PayPorter. The Board of Directors shall be in charge and responsible for the following under this policy and the relevant procedures;

- Ensure PayPorter's compliance with the obligations related to the prevention of laundering of proceeds of crime and financing of terrorism,
- Appointment of the Compliance Officer and Deputy Compliance Officer duly in accordance with the conditions specified in the relevant Regulation,

- Assess the outcomes of the risk management, monitoring and control actions and activities, and ensure the taking of necessary measures, and

- Ensure that all actions and activities are carried out with due coordination and effectively,

- Ensure that the compliance officer has the authority to make decisions with an independent will, to request all kinds of information related to their field of duty from all units within PayPorter and access them in a timely manner.

The Compliance Officer shall be responsible before the Board of Directors for taking the measures as necessary to ensure that this Policy and the relevant procedures are implemented by all staff members at the Head Office and the representation offices of PayPorter expediently and effectively and that PayPorter is not exposed to the risks related to the laundering of proceeds of crime, the prevention of the financing of proliferation of weapons of mass destruction and the prevention of financing of terrorism.

The duties, powers and responsibilities of the Compliance Officer are provided as follows:

- Carry out necessary endeavours and activities in order to ensure the Company's compliance with the obligations related to the prevention of the laundering of proceeds of crime, the prevention of financing of terrorism and the prevention of the financing of proliferation of weapons of mass destruction and the implementation of this Policy and the relevant procedures on the matter, and ensure and maintain the communication and coordination with MASAK as necessary to that end,

- Develop, update, publish and monitor and coordinate the operations in practice the procedures related to the implementation of this Policy and the relevant procedures within the organization of the Company in accordance with the Company's Policy,

- Carry out risk management, monitoring and control activities under the present Policy and the relevant procedures,

- Within the scope of this policy and related procedures; to carry out risk management and monitoring and control activities and to ensure that measures are taken for the continuous monitoring of customers and transactions, taking into account asset freezing decisions and potential matching criteria while fulfilling this duty,

- Conduct investigations on the suspicious transactions in such extent that the powers and abilities thereof allow, assess the information and findings established thereby, and report such transactions, which s/he may determine to be suspicious, to MASAK,

- Take appropriate measures to ensure and maintain the confidentiality of reports and notifications and other relevant matters.

- Keeping information and statistics on internal audit and training activities regularly and sending them to the Presidency within the specified periods,

- Reporting to the Board of Directors

- While fulfilling their duties and responsibilities, they are obliged, authorized, and responsible to act in good faith, reasonably and honestly, with impartiality and independent judgment.

Any and all staff members of PayPorter at each level and any and all employees at the respective representation offices and branches thereof shall perform and fulfil any and all their duties to ensure that this Policy and the relevant procedures are implemented expediently and effectively and that PayPorter is not exposed to the risks related to the laundering of proceeds of crime, the prevention of financing of terrorism and the prevention of financing of proliferation of weapons of mass destruction.

PayPorter and the staff members thereof shall not conduct any transaction or take any act or action, which may, in any way, be considered laundering of proceeds of crime, financing of proliferation of weapons of mass destruction and financing of terrorism or facilitate any such activity. To that end, the staff members should strictly act with due care and in due diligence in respect and through the course of their relationships with the customers against any possible laundering of proceeds of crime, financing of proliferation of weapons of mass destruction and financing of terrorism. Should they fail to do so, the staff members may encounter legal sanctions that may range from monetary fines to imprisonment.

The efficiency and adequacy in implementation of this Policy and the relevant procedures shall be subject to checks and assessments on a regular basis as a part of the internal control. This Policy shall be reviewed for at least once a year with a view to maintain its compliance with the applicable legislations in force and its conformity to the international standards.

3. DEFINITIONS

Service Risk: The risk, to which PayPorter could be exposed on account and in respect of the transactions that are not conducted face-to-face, the services rendered by the correspondent Payment Services and Electronic Money Institutions and Bank or any novel products that may be delivered through the employment of advanced technologies.

MASAK: The Financial Crimes Investigation Board, operating under the Ministry of Finance of the Republic of Turkey.

Legislations: The applicable Acts and Codes, Regulations, Communiques on the prevention of laundering proceeds of crime, financing of terrorism or financing of proliferation of weapons of mass destruction that are in force and the resolutions and instructions of MASAK.

Customer Risk: The risk of PayPorter's being abused on account of the fact that the scope of operations of the customer allows for intensive use of cash, trading of highly valuable commodities or convenient transfer of funds internationally, and that the customer or any party, who acts for or on behalf of the customer, acts with the aim of laundering of proceeds of crime, financing of terrorism or financing of proliferation of weapons of mass destruction.

Ultimate Beneficiary: Any natural person/s, who maintain/s control over the natural person, legal entity or the enterprise that lacks a legal entity, on whose behalf transactions are conducted at the counters of PayPorter, or is the actual beneficiary of the accounts held or transactions conducted by the same.

Risk: The likelihood of PayPorter's or its staff members' sustaining financial losses or loss of reputation on account of such reasons as the use of the services offered by PayPorter for the purpose of laundering of proceeds of crime or financing of terrorism or their failure to fully comply with the respective obligations thereof as imposed by the Act on Prevention of Laundering Proceeds of Crime, Prevention of the Financing of Proliferation of Weapons of Mass Destruction and Prevention of the Financing of Terrorism and the regulations and communiques issued pursuant to such act.

Laundering Proceeds of Crime (Money Laundering): The transactions aimed at the inclusion of the proceeds derived from illegal means to the financial system and particularly the transformation of the same into another form than cash and getting the same through a course within the financial system and legitimization of such proceeds by way of changing the identity of the same in order to create the false impression that such proceeds have, in fact, been derived through legal means.

Financing of Terrorism: Funding a terrorist or a terrorist organization in order for such funds to be used entirely or partially for the conduct of such acts that are provided by the law to be criminal offenses or deliberately funding such a terrorist or terrorist organization, knowing that the same shall be used for such purposes or even without association with a specific act.

Weapons of Mass Destruction: Anti-personnel weapons that can cause large amounts of destruction on living beings, including humans (Chemical, biologic, radioactive and nuclear weapons).

UNSC: United Nations Security Council,

UNSC Resolutions: Sanctions imposed by the United Nations Security Council on preventing the financing of the proliferation of weapons of mass destruction and their annexes;

FATF: Financial Action Task Force,

AML: Anti Money Laundering (Prevention of Laundering of Proceeds of Crime),

Compliance Program: All measures to be established in order to prevent the laundering of proceeds of crime and the financing of terrorism, as set out in Article 5,

Politically Exposed Person (PEP): Senior executives and members of the board of directors of international organizations who are entrusted with a significant public function by election or appointment abroad or in a foreign country mean other persons holding functions equivalent to those of their senior executives.

Compliance Officer: The Compliance Officer, who has been assigned within the organization of PayPorter under The Law on the Prevention of the Proceeds of Crime, and the other applicable regulations in force, enacted on the basis of

the said Law, and who is in charge of ensuring and authorized to ensure the compliance of the Company with the respective obligations thereof that arise out of such legislations.

This Policy and Related Procedures: The entirety of the measures developed within the organization of the Company and in accordance with the Company's Policy for the purpose of the prevention of the laundering of proceeds of crime and the prevention of financing of terrorism

Country Risk: The risk, to which PayPorter may be exposed on account of its relationships with the citizens, companies or financial institutions of those countries that do not have adequate regulations in force on the prevention of laundering of proceeds of crime or financing of terrorism or financing of proliferation of weapons of mass destruction do not cooperate at adequate level for combating the said offenses or are considered risky by international organizations, which are identified in accordance with the applicable legislations, or the transactions that could be conducted through the course of such relationships.

Remote Communication Tool: It refers to all types of tools or media that allow the establishment of a contract without physical confrontation, such as letters, catalogues, telephone, fax, electronic mail messages, Internet and SMS services.

4. RISK MANAGEMENT

4.1. Purpose and Scope of Risk Management

The main purpose of the risk management policy is to identify, assess, rate, monitor and mitigate the risks that PayPorter may be exposed to in relation to the risks of laundering proceeds of crime, proliferation and financing of weapons of mass destruction and terrorist financing, as well as the risks of violation, non-implementation and avoidance of asset freezing decisions within the scope of the Law on Prevention of Financing the Proliferation of Weapons of Mass Destruction.

In line with the primary objective of its Risk Management Policy, PayPorter has established written procedures to manage the risks it may be exposed to in the areas mentioned above. These procedures detail the monitoring and control activities to be carried out for the assessment, monitoring, and mitigation of such risks, as well as the specific measures to be taken and the controls to be implemented.

PayPorter's risk management policy ensures that appropriate processes and systems are established and function effectively to identify, classify, assess, and mitigate legal non-compliance risks arising from non-adherence to the obligations stemming from the legislation that forms the basis of this policy, as well as customer, service, and country risks.

Monitoring and control activities established within the scope of the Company Compliance Policy are designed to continuously monitor customers and their transactions in order to manage the risks listed above.

4.2. Customer Acceptance Principles of the Company

The customer portfolio of PayPorter is composed of such customers, who:

- Shall maintain the company-customer relationship straightforwardly and honestly on the basis of mutual trust,
- Observe the applicable acts and codes as well as ethical codes through the course of their operations and their relations with the Company,
- Are not engaged or involved in the laundering of proceeds of crime, financing of terrorism and weapons of mass destruction,
- Does not avoid delivering the required information and documents requested by the Company under the applicable legislations timely and in compliance with the relevant procedures, and
- Are appropriate, effective and of satisfactory quality in respect of the purposes and goals of the Company.

The main principles implemented by the Company in respect of the acceptance of customers are provided as follows;

- In the event that a permanent business relationship is requested to be established or our Company services are requested to be used; the following points should strictly be observed by our staff members.

- The customer accounts shall be opened for the real full name or trade name of the customer. Any account may not be opened using another name, an anonymous name, or nickname.

- It is strictly forbidden to accept customers, who want to establish or maintain a permanent business relationship under such names that are obviously untrue. Any customer name registered on the system may not consist of points (consisting of symbols such as numbers or punctuation marks only to indicate who the customer is), or other forms of actual account holders and methods for hiding or concealing their identity.

- Any persons and entities, who are hesitant to provide information or who provide misleading information that cannot be confirmed, may not be accepted as customers. Clarity and transparency should be ensured in respect of the customer transactions and information.

- The opening of accounts for such persons, who file a request to become a customer without face-to-face contact via such means as mail, e-mail, the Internet, phone etc., shall primarily require, as a principle, meeting with the customer or the legal representative of the same face-to-face and obtaining from the same the required information and documents for identification.

- In the event of strong suspicion, information or document suggesting that the financial assets of the person or entity, with whom a business relationship or customer relationship is proposed to be established, have not been gained through legal means; such proposed business relationship shall not be established.

- Any request by any third party to open accounts on behalf of any person/s (excluding the accounts to be opened on behalf of such persons, who are under custody and guardianship, or of minors) shall not be fulfilled unless such third party substantiates on documentary basis that s/he has been expressly authorized by the represented customer to do so and states the purpose and necessity to open account.

- The powers of attorney to be submitted for such purposes shall strictly be required to be have been certified by a notary public. In the cases, where the customer cannot be identified sufficiently in the applications filed by the respective representatives thereof, the customer's identity shall be had confirmed by the entity that has issued the relevant document.

- Any person or entity, who or which is established to be on the lists issued by the relevant public authorities as a part of combating the laundering of proceeds of crime, financing of terrorism and financing of proliferation of weapons of mass destruction in Turkey, shall not be accepted as a customer. In the event any person or entity is established to be on any such list in the aftermath of the establishment of a customer relationship, a report shall be filed to the Compliance Department in respect of such person or entity.

- In the cases, where the potential customer cannot be identified in accordance with the applicable legislations or satisfactory information cannot be obtained on the purpose of the potential business relationship; the business relationship shall not be established and the transactions requested by the customer shall not be performed unless the reservations and deficiencies on the matter are eliminated.

- In the cases, where the customer cannot be successfully identified and verified as necessary due to any suspects in respect of the adequacy and the accuracy of the previously obtained customer identification details; the business relationship shall be terminated.

- Necessary and appropriate measures shall be taken in order for not to establish business relationships with such prohibited persons and entities, who or which are listed within the lists that have been issued by the United Nations Security Council for the prevention of financing of terrorism and financing of proliferation of weapons of mass destruction that are also binding on Turkey and such other similar international lists, which are required to be taken into consideration by the entities within the international financial system as well as the financial institutions operating in Turkey, and shall be implemented diligently.

- Any business relation shall strictly not be established with Shell Banks.

- The Company decides to which of the customers and for which types of services it will offer the possibility of conducting transactions via a remote communication tool based on the results of the risk assessment it conducts, taking into account such issues as the type and nature of the payment transactions to be conducted, the magnitude of the financial and non-financial impact, if any, the maximum transaction amount, and the reliability of the customer. Depending on the results of the risk assessment, the Company may decide to execute the payment transaction in the simultaneous physical presence of the parties.

- During the identification and establishment of the contractual relationship through remote communication tools, the Company meets the minimum requirements set forth in Article 22 of the Communique on Information Systems of Payment and Electronic Money Institutions and Data Sharing Services of Payment Service Providers in the Field of Payment Services.

4.2.1. Correspondence Relations with Other Financial Institutions and Payment Institutions

Necessary and appropriate measures shall be taken under the applicable legislations in order to accurately identify and assess the nature and level of the risks, which the financial institutions, with which the Company maintains correspondence relations, in the aspects of money laundering, financing of terrorism and financing of proliferation of weapons of mass destruction. Some of such measures include the following;

- Assess anti-money laundering and terrorist financing system of the correspondent financial institution, and ascertain that the system is appropriate and effective,
- Authorized by the delegacy of the country where the counterparty financial institution is located,
- Obtain, by making use of publicly available resources, reliable information on whether the correspondent financial institution has been subject to any investigation for money laundering or financing of terrorism or financing of proliferation of weapons of mass destruction and been punished, its business field, reputation and the adequacy of inspection on it,
- The adequacy of the AML system that is in place in the country, where the correspondent institution is based, should be assessed with due consideration of the FATF country assessment reports and the other reliable sources.
- It is a strict requirement to obtain approval from the Compliance Officer in advance of the establishment of any new correspondent relationships.
- The responsibilities of each of the Company and the correspondent financial institution should be identified and set forth clearly within a contract to be executed.

4.3. "Know Your Customer" Principle

The basis of PayPorter's customer acceptance policy with regards to the prevention of laundering of proceeds of crime, proliferation of weapons of mass destruction and financing of terrorism is laid by the "Know Your Customer" principle. Accordingly; in order for protection from the persons and acts that are involved or that involve laundering of proceeds of crime, financing of terrorism and financing of proliferation of weapons of mass destruction PayPorter attaches the utmost importance to the "Know Your Customer" principle and shall adopt and implement a policy on the matter that is in conformity to the relevant international standards and in compliance with the applicable legislations.

As a part of and in line with the "Know Your Customer" principle, necessary and appropriate measures shall be taken in accordance with the applicable legislations and the Company on the following matters;

- Identification of the customer,
- Knowing the ultimate beneficiary,
- Obtaining adequate information about the purpose and nature of the requested transaction,
- Monitoring the status and transactions of the customer through the course of the customer relationship,
- Taking necessary and appropriate measures in respect of the customers, activities and transactions that require special attention.

Measures are taken in accordance with applicable legislations, best practices and the Company's policies and procedures.

PayPorter attaches the utmost importance to the "Know Your Customer" principle in order to protect itself from the offenses of laundering of proceeds of crime, financing of terrorism and financing of proliferation of weapons of mass destruction. To that end;

- PayPorter takes additional measures that are compliant with the FATF requirements for the continuous monitoring of certain transactions and the business relationships and transactions with the natural persons or

legal entities from such countries, with which there are no existing or ongoing cooperation, or which are non-compliant or non-eligible, or which considered to be inadequate. Any and all transactions conducted with natural persons or legal entities from such countries shall be subjected to special review.

- Any potential customer, who requests to open payment accounts and procure payment services, shall be checked against the Company's respective in-house list and the international sanction lists (such as OFAC, EU, UN, HMT, FATF and PayPorter's black list). The said checks shall be conducted also during the opening of payment accounts and the rendering of money transfer and payment services.

- Under Law No. 6415 on the Prevention of the Financing of Terrorism and Law No. 7262 on the Prevention of the Financing of the Proliferation of Weapons of Mass Destruction, this entity conducts work to identify, assess, monitor, and mitigate the risks of violating, failing to implement, or evading asset-freezing decisions, and applies enhanced controls to enforce these sanctions.

- PayPorter's policies requires it to obtain full and comprehensive information about the outgoing and incoming electronic money transfer orders, including the names of the sender and the recipient as well as the addresses and the account numbers of the same and the purpose of transfer.

- The Politically Exposed Persons (PEP) are the persons, who a who has been entrusted with a prominent public function, such as Presidents or Heads of Government, senior level politicians and senior governmental, judicial or military officials. The senior executives of state-owned enterprises, officials of prominent political parties, the family members of PEPs (first degree family members such as parents, spouses and children etc.) or the business partners of the same also pose similar reputation risks to those posed by PEPs themselves. PEPs are in the high-risk customer group, and their account opening process as well as the transactions that are conducted on such accounts after the opening of the same shall be subject to review by the Compliance Department.

4.3.1. Identification

PayPorter requires the establishment of a permanent business relationship with customers and, if necessary, the implementation of a transfer transaction for customers who do not have a permanent business relationship or the provision of payment services to customers; in accordance with the applicable legislation on the identification and confirmation of the customer (Regulation on Measures Regarding Prevention of Laundering Proceeds of Crime And Financing of Terrorism / Chapter Three (Article 5-Article 17)) in compliance with this policy and company procedure on the subject (07.010.P03 Customer Identification Procedure) is to be done in a timely, complete and accurate manner.

Identification of the customer; The provision, detection, control and verification of the customer's identity information is carried out by the applicable legislation (Regulation on Measures Regarding Prevention of Laundering Proceeds of Crime and Financing of Terrorism / Chapter Three (Article 5-Article 17)) and by carrying out the necessary work and transactions within the Company's Policy and procedures.

- In the case of a permanent employment relationship, regardless of the amount in question, information shall be obtained about the purpose and nature of the employment relationship,

- In the cases, where the amount of transaction or the sum of the amounts of multiple linked transactions is equal to or in excess of the amount specified in the applicable legislation, (TL or equivalent foreign currency)

- In the cases of wire transfer transactions, where the amount of transaction or the sum of the amounts of multiple linked transactions is equal to or in excess of the amount specified in the applicable legislation, (TL or equivalent foreign currency)

- Irrespectively of the amount at issue in the cases that require suspicious transaction reporting, and

- Irrespectively of the amount at issue in the cases, where there is suspicion in place as to the adequacy and the accuracy of the previously obtained customer identification details,

- The customers and the persons, who act for or on behalf of the customers, shall be identified by way of obtaining the identification details of the same and the verification of the accuracy of such details in accordance with the applicable legislations.

Reliance on third parties; PayPorter can establish business relationships or carry out transactions by relying on measures taken related to the customer by another financial institution on identification of the customer, the person acting on behalf of customer and the beneficial owner, and on obtaining of information on the purpose of business relationship

or transaction. In that case, the ultimate responsibility shall be assumed and borne by PayPorter under the Act and the related regulations.

- Third parties have taken measures to meet the requirements of customer identification, record keeping and the "know your customer" principle, and are also subject to effective regulations and supervision in conformity to international standards in combating money laundering and financing of terrorism they should be are resident abroad,

- Certified copies of the documents related to identification (in case a permanent business relationship is established through remote identification by the trusted organization, the digital images taken) will be provided immediately from the third party upon request,

- Provided that the third party ensures that the identification of the customer whose information is shared is not made under simplified measures.

- In the cases, where a third party is relied upon and a business relationship is established with the same, the identity details shall be obtained immediately from such third party.

- The principle of reliance on third parties shall not be applicable in the cases, where the third party is resident in a risky country.

- The approval of the Compliance Department must be obtained prior to the execution of the transaction in connection with the principle of reliance on third parties.

The approval of the Compliance Department should be obtained prior to the conduct of any transaction that involves the principle of reliance on third parties, and also the identity details of the customer should be obtained from the third party immediately in the event of the establishment of a business relationship or the conduct of a transactions by way of reliance upon the third party.

4.3.2. Know the Ultimate Beneficial Ownership

Necessary and appropriate measures shall be taken and implemented carefully in accordance with the applicable legislations in order to establish and identify the actual beneficiary in the case of the establishment of a continuous business relationship and the conduct of the requested transactions.

Where the person requesting the transaction declares that he or she is acting on behalf of another person, the identity and authorization status of the person requesting the transaction and the identity of the person on whose account the transaction is being acted shall be determined in accordance with Articles 6 to 14 of the applicable regulation.

In cases where there is a suspicion that an individual is acting on behalf of another person, even if they declare they are not, our Company implements measures to identify the ultimate beneficial owner. As part of this process, in order to remind individuals acting on their own behalf but for the benefit of another, necessary announcements are posted in a clearly visible manner at our Company's branches and representative offices.

4.3.3. Continuous Monitoring of Customers and Transactions

The process of assessment of the customers in terms of the laundering of proceeds of crime and the risks associated to the same shall not be limited only to the customer acceptance step. The relations and transactions of customers should be monitored continuously. To that end;

- In the cases where the information and documents used for the identification of the customers are no longer valid, such information and documents shall be renewed.

- Due attention should be taken to make sure that that the transactions conducted are in consistent with the declared or known business operations of the customer; and in the case of any such transaction that is not so consistent, the customer shall be required to produce and submit papers or documents that would constitute proof and substantiate the rationale for the proposed transaction.

- Special attention shall be paid to complicated transactions with an extraordinarily large size and to such transactions that do not appear to be serving a reasonable legal and economic purpose, and adequate information shall be required from the customer about the purpose of the transaction, which is requested to be

conducted. Should adequate information cannot be obtained from the customer in the cases of suspicion, the transaction shall not be exercised or, if it has already been exercised, the Compliance Department shall be notified of the matter immediately. The information, documents and records obtained from customers for such transactions shall be retained for a period of 10 years in accordance with the "Obligation to Retain and Submit".

- In the cases, where there are any suspects in respect of the adequacy and the accuracy of the previously obtained customer identification details; the identification and the verification of identity shall be repeated, and if the same cannot be so repeated, the business relationship shall be terminated.

- It shall be continuously monitored whether or not the accounts opened by third parties on the basis of power of attorney are used by/ on behalf of the actual holders of such accounts, and due care shall be taken in order to make sure that the accounts opened are used for the declared purposes. Although the transaction considers the general rules of law for the use of indefinite powers of attorney, it is also important to keep the information and identification documents up-to-date.

- The necessary reviews shall be conducted by the Compliance Department in order for the minimization of the risk for the newly launched products and the abilities introduced by technological advancements to be used for the purpose of money laundering and financing of terrorism.

- Special attention shall be paid to such transactions, which are performed through the systems that enable performing distant transactions without having to appear in person, and such transactions, which are not compatible with the financial profile and the operations or are not related to the operations of the customer, shall be monitored closely, and in the event of the detection of any discrepancy, the Compliance Department shall be notified of the same.

According to the "know your customer" guidelines and PayPorter's customer acceptance principles as set forth within Article 4.2 hereof; the account activity, details and documents, the general conduct and the transaction requests of the customers, who are in a permanent business relationship with the Company, should be monitored strictly by the staff members and the manager of the relevant branch/ representation office and the Compliance Department should be conducted in the event of the emergence of any suspicion.

Also, the transactions conducted by such customers, who are not in permanent business relationship with but also procure transfer/payment services from PayPorter, shall also be assessed with respect to the foregoing matters.

The profile of each customer in terms of money laundering and financing of terrorism shall be developed as a part of the monitoring and control activities with due consideration of the profession, business history, activities, financial standing, account and transactions as well as the country of residence/operation and the like up-to-date information and indicators. The customers, business relations and transactions that pose a high risk shall be identified, and be monitored through the monitoring and control processes and systems by way of the risk management framework developed.

4.3.4. Taking Necessary and Appropriate Measures in Respect of the Customers, Activities and Transactions That Require Special Attention

The necessary and appropriate measures shall be taken according to the applicable legislations and the Company's Policy and procedures on such matters as those provided below, which require special attention:

- Relations with the correspondent institutions, with which any business relationship is established, and risky countries,

- Wire transfers,

- Transactions of customers with a contract has been established through remote communication and whose identity has been identified and confirmed,

- The business relationships, about the purpose of which adequate information cannot be obtained,

- Any other types of customers, activities and transactions, in respect of which special attention is recommended by the FATF to be paid in terms of the laundering of proceeds of crime and financing of terrorism,

- Politically Exposed Persons (PEP) and their family members (first-degree relatives like parents, spouse, and children) or their business partners and their businesses and transactions.

4.4. Prevention of the Financing of Proliferation of Weapons of Mass Destruction and Freezing of Assets

At PayPorter, the assessment of customers for potential financing of proliferation of weapons of mass destruction and related risks is not limited to the customer on boarding stage. Customer relationships and transactions are continuously monitored.

Within the scope of Law No. 6415 on the Prevention of Financing of Terrorism and Law No. 7262 dated 27/12/2020 on the Prevention of Financing the Proliferation of Weapons of Mass Destruction and Law No. 7262 dated 27/12/2020 on the Prevention of Financing the Proliferation of Weapons of Mass Destruction, studies for the identification, evaluation, monitoring and mitigation of the risk for the risks of violation, non-implementation and avoidance of asset freezing decisions and advanced controls for the implementation of such sanctions are applied. In these monitoring and control activities, measures are taken to continuously monitor customers and their transactions by taking into account asset freezing decisions and potential matching criteria.

Upon the publication in the Legal Gazette of the asset freezing decisions taken pursuant to the provisions of Law No. 6415 and Law No. 7262 and the decisions regarding the lifting of these decisions and the receipt of the notification regarding these decisions by our Company, these decisions are immediately put into practice within the scope of our Company's Procedure No. 07.010.P05 on Prevention of the Financing the Proliferation of Weapons of Mass Destruction and Freezing of Assets.

4.5. Risk Management Activities

4.5.1. General Risks That Could Be Encountered

Utmost care should be taken for compliance with the principles, rules and guidelines as provided within MASAK regulations and set forth within this Policy in order to prevent the conduct of any transactions by launderers of proceeds of crime and those, whose intention is to finance terrorism and proliferation of mass destruction weapons through PayPorter and to file suspicious transaction reports in the event of the occurrence of any such situation. In the event of any failure in such compliance, PayPorter and the staff members thereof may be encounter and be exposed to the following risks.

4.5.2. Legal Risk

The legal risk means the likelihood of PayPorter's standing or operations being affected adversely on account of the initiation of any legal actions against PayPorter or due to the contracts executed. Financial institutions are exposed to serious legal risks in the event and on account of their failure to fulfil their obligations imposed for the purpose of combating money laundering, and in some countries, even their licenses could be revoked in the event of continued violation of or failure in the fulfilment of the relevant obligations.

In order to minimize the above-mentioned risks for PayPorter and PayPorter employees and representatives, the legal regulations on the subject are regularly monitored by the Compliance Department of the Company and the necessary information is provided to the relevant parties (PayPorter’s employees, branches and representatives) by the appropriate method. This information also covers changes and updates to be made in the Company's Compliance Policy.

4.5.3. Reputation Risk

Financial institutions base their operations on trust, on which account the public opinion about the integrity of and the customers' trust in PayPorter are one of the most valuable assets PayPorter can have. The reputation risk means the existing and potential effects of the negative opinions in the public about PayPorter on the operations and the income of PayPorter. The reputation risk may impede PayPorter's opportunities to enter into new business relations and may also affect the maintenance of the existing business relations thereof.

The reputation risk is not limited merely to national territories. Article 21 of the 40 Recommendations issued by FATF of which Turkey is also a member, provides as follows; "Financial institutions should give special attention to business relationships and transactions with persons, including companies and financial institutions, from countries which do not or insufficiently apply the FATF Recommendations." As far as the financial system is concerned, the foregoing recommendation suggest that the reputation of the financial institutions that are based in a non-compliant country is impaired before other countries and that the transactions conducted by foreign financial institutions through the agency of the financial institutions based in a non-compliant country undergo more bureaucratic processes, which leads to delays in a further extent.

4.5.4. Operational Risk

The operational risk the one risk, to which PayPorter and PayPorter's employees are mostly likely to be exposed, and means the risk of PayPorter's sustaining losses directly or indirectly on account of ineffective internal control procedures

or external factors. Most of the operational risks are related to PayPorter's weaknesses about the fulfilment of its obligations.

In order to minimize of the foregoing risks for PayPorter and PayPorter's staff members; certain risk management activities, the main elements of which are provided as follows, are carried out with a view to ensure that PayPorter is protected from the acts of financial fraud, laundering of proceeds of crime and financing of terrorism and financing of proliferation of weapons of mass destruction and is positioned as a reliable financial institution in the national and the international domains.

The scope of the risk management activities encompasses, at minimum level, the following activities:

- Development of risk identification, rating, classification and assessment methods in respect of and based on the customer risk, the service risk and the country risk,
- Rating and classification of services, transactions and customers with respect to the associated risks,
- Monitoring and checking and controlling of risky customers, transactions and services and reporting of the same to give alerts to the relevant units; development of appropriate operational and control rules in order to make sure that transactions can only conducted after being approved by the immediately superior authority and are audited where necessary,
- Retrospective examination of the consistency and efficiency of risk identification, assessment, rating and classification methods on the basis of precedent cases or transactions conducted, and the re-assessment and revision of such methods with respect to the conclusions drawn and the emerging circumstances,
- Keeping track with the national legislations and the recommendations, principles, guidelines, standards and guides developed by international organizations regarding the matters that fall to the scopes of risks and carrying out development endeavours as necessary on the same, and
- Reporting of the outcomes of the risk monitoring and assessment activities to the Board of Directors on a regular basis.

The risk management activities related to the implementation of the Company's Compliance Program shall be designed by the Compliance Officer in accordance with the provisions of the applicable legislations and this Policy, and be carried out within the organization of the Compliance Department.

4.5.5. Risks That Could Be Encountered Due to the Customers and Customers' Transactions/ Operations

The risks of laundering and financing of terrorism/proliferation of weapons of mass destruction, which PayPorter could encounter and to which it could be exposed due to the customers and customers' transactions/ operations, are classified into three main groups as follows in accordance with the applicable legislations;

- Customer Risk,
- Service Risk,
- Country Risk.

The customer, service and country risks related to money laundering, financing of terrorism and financing of proliferation of weapons of mass destruction shall be assessed with due consideration of the following basic criteria:

- Level of knowledge about the market position and the operations of the customer, and the nature of information known,
- Value of the customer in possession of and/or the volume of the transactions conducted thereby through or at the counters of PayPorter,
- The purpose and nature of the customer's relationship with PayPorter,
- The level of accordance and adequacy of the country, and/or territory, where the customer operates, and/or the regulatory and supervisory practices regarding money laundering and financing of terrorism, to which the customer's operations are subject,
- The duration and the course of the customer's existing relationship with PayPorter,

- The type and nature of the products and services used by the customer,

The customers shall be included to the appropriate risk criteria, both at the commencement and through the course of the customer relationship, with respect to the nature and scope of their operations as well as their relations and transactions with PayPorter and in accordance with and on the basis of the aforementioned criteria and any other customer-specific information and criteria if any. Through the course of the determination of the risk category, into which the customer is to be categorized; the customer, service and country risks connected to the customer, the financial transactions conducted thereby and the financial products and services used by the same shall be taken into consideration and assessed as a whole.

While the customers, which are categorized into the medium and low risk categories, and the transactions thereof shall be subjected to PayPorter's relevant standard monitoring, checks and controls; the customers, which are categorized into the high-risk category, and the transactions thereof shall be monitored closely through the expedient monitoring and control methods.

In respect of the customers, which are categorized into high-risk category in relation to the service and country risks; reinforced know-your-customer principle (tightened measures) shall be implemented. Accordingly; the central monitoring and control activities carried out through a risk-based approach within the organization of the Compliance Officer shall be designed and implemented in such manner that they mainly focus on the customers and transactions within the high-risk category.

The customer groups and the products and services that fall to the high-risk category shall be identified by the Compliance Officer through a risk-based approach in accordance with the applicable legislations and this Policy, and be so subjected to the appropriate and effective monitoring and controls with respect to the characteristics thereof.

In respect of the groups, which are identified to be posing high risk as a result of the risk rating endeavour; the following minimum additional measures shall be taken with a view to ensure the mitigation of the risk to be undertaken:

- Development of procedures for continuous monitoring of transactions and customers,
- Requirement of the approval of the immediately higher-level official for the establishment of a business relationship, the maintenance of an ongoing business relationship or the conduct of a transaction,
- Procurement of as much information as possible about the nature of the business relationship, the purpose of the transaction and the origin of the assets, being the subject matter of the transaction, and
- Procurement of additional information and documents as a part of customer due diligence (know-your-customer) efforts, taking additional measures regarding the verification and documentary substantiation of the information submitted, and more frequently updating the identity details of the customer and the actual beneficiary.

The risk categories of the customers shall be identified in accordance with the applicable legislations and the international norms in the light of their identity details, our company products they use, scopes of operations and other customer information available.

Accordingly;

- The persons and the entities, for whom and which special attention is required by the FATF's recommendations to be paid,
- The persons and the entities, who and which are considered necessary to be monitored closely for being resident in or related to risky countries or territories,
- The persons and the entities, who and which are engaged in such operations that are considered highly risky under the international norms in terms of laundering of proceeds of crime, financing of terrorism and financing of proliferation of weapons of mass destruction (such operations that involve intensive use or transfer of cash/ foreign exchange, trading of highly valuable commodities and assets etc.), and
- The persons and the entities, who and which predominantly use any PayPorter service that is considered to be risky and objectionable by the competent legal authorities in terms of their relation to the laundering of proceeds of crime, financing of terrorism and financing of proliferation of weapons of mass destruction and other financial offenses, and is, thus, considered by the same necessary to be closely monitored, and that falls to the scope of high risk category, as well as such other customers, which are to be considered risky in respect of the current natures and the scopes of operations thereof or the nature of their relations and transactions with PayPorter within the framework of the risk management, monitoring and control activities under this Policy and related

procedures that are to be implemented in accordance with the international norms, the applicable legislations and the provisions of this Policy, and for which it is considered necessary to pay special attention, shall be monitored within the high risk category.

As far as the service risk is concerned;

- Wire transfers,
- The systems, which enable the conduct of transactions in other forms than face-to-face conduct, (Individuals identified through remote communication tools and customers who are parties to established contracts are monitored under a different risk profile),
- The products and services based on new, emerging and advanced technologies,
- The business activities and transactions, the ultimate beneficiary of which cannot be identified fully and clearly,
- Such other product, service and transaction types, which are to be considered risky in respect of the natures thereof within the framework of the risk management, monitoring and control activities under this Policy and related procedures that are to be implemented in accordance with the international norms, the applicable legislations and the provisions of this Policy, and for which it is considered necessary to pay special attention, shall be monitored within the high risk category.
- Within the scope of the payment instrument acceptance service under subparagraphs (a) and (b) and subparagraph (c) of the first paragraph of Article 12 of the Law on Payment and Securities Settlement Systems, Payment Services and Electronic Money Institutions dated 20/6/2013 and numbered 6493, the measures in subparagraphs (a) to (f) of the first paragraph shall be applied as a minimum in the payment service (virtual terminal service) performed through the terminal provided by the payment institution, the establishment of a business relationship with the customer (merchant) and other transactions requiring identification.

The countries and territories, which are described below, and the customers, which are based in or related to such countries and territories, shall be monitored closely within the high country risk category:

- The countries, which the FATF has advised to the member countries to be posing risk in terms of the laundering of proceeds of crime and financing of terrorism and in respect of which FATF has advised to the same to take additional measures,
- The countries listed on the "Risky Countries" risk as announced by the relevant Ministry,
- The countries, which are subject to sanctions at international level under the resolutions of the United Nations Security Council on account of their policies and practices related to the laundering of proceeds of crime, financing of proliferation of weapons of mass destruction and financing of terrorism,
- The countries, which have been announced by the European Union or OFAC to be posing high risk in terms of the laundering of proceeds of crime, financing of proliferation of weapons of mass destruction and financing of terrorism.
- Extraterritorial centers, free trade areas and financial centers,
- Tax havens, and (off shore centers)
- The countries, which lack adequate regulations regarding the prevention of laundering of proceeds of crime, financing of proliferation of weapons of mass destruction and financing of terrorism.

4.6. Monitoring and Control

4.6.1. Purpose and Scope of Monitoring and Control

The main purpose of monitoring and control is to protect PayPorter from risks and to continuously monitor and control whether or not the operations of PayPorter are carried out in compliance with the applicable legislations and in accordance with the relevant policies and procedures in force.

Monitoring and controls shall be established and implemented through a risk-based approach. Accordingly; appropriate monitoring and control methods shall be developed with respect to the customers, transactions and the services of the Company, and shall so be implemented effectively.

4.6.2. Monitoring and Control Activities

The monitoring and control activities shall be designed and implemented through a risk-based approach under the supervision and through the coordination of the Compliance Officer in compliance with the applicable legislations and in accordance with the provisions of this Policy. Accordingly; in addition to the standard controls applicable for all operations of PayPorter, appropriate and effective control processes, systems and methods shall be identified and implemented for more closely monitoring of the customers, transactions and activities, which are considered highly risky and for which special attention should be paid.

The monitoring and control activities mainly include the following:

- The monitoring and control of the customers and transactions that fall to the scope of high risk category,
- The monitoring and the control of the customers that are classified as PEP,
- The monitoring and control of the transactions that are conducted with risky countries,
- The monitoring and control of complex and extraordinary transactions,
- Control by way of sampling of the transactions, the amounts of which exceed the predefined amounts, in terms of consistency with the customer profile,
- The monitoring and control of linked transactions, the amount of which exceeds the amount that requires identification,
- Control of the compliance, adequacy and currency of the existing information and documents of the customer, and procurement of complementation of any missing information or document,
- Continuous monitoring of the consistency of the customer transactions with the information about the business, risk profile and fund sources of the relevant customers throughout the entire duration of the business relationship, control of the such transactions, which are conducted through the systems that enable performing distant transactions without having to appear in person (Transactions of individuals identified through remote communication tool and customers who are parties to the contracts they establish,)
- Risk-oriented control of the services, which could be exposed to and vulnerable to risks and abuse in terms of money laundering, financing of terrorism and proliferation of weapons of mass destruction due to new products and technological advancements, and
- Within the scope of Law No. 6415 dated 07/02/2013 on the Prevention of the Financing of Terrorism and Law No. 7262 dated 27/12/2020 on the Prevention of the Financing of the Proliferation of Weapons of Mass Destruction, measures are taken to ensure the continuous monitoring of customers and transactions in the context of monitoring and control activities aimed at addressing the risks of violation, non-implementation, or circumvention of asset freezing decisions. These measures are implemented by taking into account the asset freezing decisions and potential match criteria.
- Any other monitoring and control activities that could be carried out within this scope.

The central monitoring and control activities shall be carried out within the organization of the Compliance Department.

4.7. Training

4.7.1. Purpose and Scope of Training Policy

The scope of the training policy, which is applicable to all staff members of PayPorter, is to develop PayPorter's corporate culture and awareness about the risks related to money laundering and financing of terrorism as well as PayPorter's legal obligations, Policy, procedures and practices on the same, and to furnish the staff members with up-to-date knowledge on the matter.

4.7.2. Training Activities

PayPorter's training activities aimed at the prevention of laundering of proceeds of crime, financing of terrorism and financing of proliferation of weapons of mass destruction shall be designed to cover all relevant staff members in compliance with the applicable legislations and in accordance with the provisions of this Policy, and shall be so carried out under the supervision and through the coordination of the Compliance Officer. The training program shall be prepared annually by the Compliance Officer with the participation of the relevant departments of PayPorter. The effective implementation of the training program shall be supervised by the Compliance Officer.

The contents of training shall be customized with due respect to and on the basis of the term of service, title and the position of the relevant staff members, and it shall be ensured that each staff member is provided with appropriate trainings on a regular basis, accordingly. The training contents shall be updated and revised as necessary on a timely basis with respect to the amendments to the applicable legislations and the other developments on the matter.

The contents of the trainings that shall be provided to the staff members shall be designed and developed to include the following at minimum:

a) The concepts of laundering of proceeds of crime and financing of terrorism,

b) The phases and methods of laundering of proceeds of crime and case studies on the matter,

c) Applicable legislations regarding the Laundering of Proceeds of Crime and Financing of Terrorism,

d) In accordance with the Act No. 5549 and the relevant regulations;

- **a.** Customer due diligence (know-your-customer),
- **b.** Suspicious transaction reporting,
- **c.** Submission of information and documents,
- **d.** Retention and submission,
- **e.** Obligations to provide information and documents, and sanctions to be imposed in the event of failure in the fulfilment of such obligations, and

e) Enforcements to be applied in case of non-compliance with obligations,

f) The international regulations in the field of combating money laundering, financing of terrorism and financing of proliferation of weapons of mass destruction.

The accordance and fitness for the needs and the adequacy of the trainings are monitored and assessed closely. The training activities shall be reviewed with the participation of the relevant units with respect to the results of the measuring and evaluation activities, and shall be repeated on a regular basis as needed.

The results of any and all training activities carried out shall be retained for submission during the audits to be conducted.

a) Training dates,

b) Regions or provinces, where training activities have been carried out,

c) Training method,

d) Total duration of training in hours,

e) Number of staff members, to whom training activities have been carried out,

f) Distribution of the staff members, to whom training activities have been carried out, by the units and titles,

g) Training contents,

h) Titles and fields of specialization of the instructors.

4.8. Miscellaneous Provisions

4.8.1. Detection and Reporting of Suspicious Transactions

Pursuant to the provisions of Article 4 of the Act No. 5549 on the Prevention of Laundering of Proceeds of Crime and Article 27 of the Regulation on Measures; in the event of any information, suspicion or reasonable grounds to suspect that the derivation through illegal means of the assets, being the subject matter of any transaction that has been conducted or attempted to be conducted at the counter of the Company or through the agency of the Branches/ representation offices thereof, any such transaction shall be reported to the Compliance Officer via mail irrespectively of the amount of such transaction.

The Compliance Officer shall, thereupon, conduct the necessary investigation about the suspicious transaction report and file a report to the Financial Crimes Investigation Board, the Ministry of Finance of the Republic of Turkey within the legally prescribed period of time.

4.8.2. Definition of Suspicious Transaction

A suspicious transaction is a case where there is any information, suspicion or reasonable grounds to suspect that the assets, which are subject to the transactions conducted out or attempted to be conducted at the counters of or through the agency of PayPorter, has been acquired through illegal means or used for illegal purposes and is used, in this scope, for the acts of terrorism activities or by terrorist organizations, terrorists or those, who finance terrorism or proliferation of weapons of mass destruction.

The definition of suspicious transaction also includes the use for illegal purposes of the assets, being the subject matter of the relevant transaction, as well as the acquisition of the same through illegal means, whereby the prevention of the financing of terrorism (including connection to the same) and the proliferation of weapons of mass destruction is aimed.

The existence of suspicion or reasonable grounds to suspect shall be assessed by way of the examination of multiple transactions where necessary.

Our Company utilizes automated alert systems and software for the identification of suspicious transactions. These systems have been implemented to mitigate the risks our Company may encounter while conducting its operations. By integrating parameters related to money laundering, terrorist financing, and the financing of the proliferation of weapons of mass destruction into these systems, they contribute to the prevention of risks in this area.

Considering the fact that the element of suspicion cannot be defined with parameters in terms of many suspicious transactions and customer profiles, and that sometimes the suspicion arises not from the transaction but from the behavior and actions of the customer making the transaction, solutions enabling internal reporting have been developed within our Company so that system users who have a one-to-one relationship with the customer can also report.

4.8.3. What is Suspicious Transaction Reporting

Suspicious transaction reporting is a type of reporting that countries are required to implement compulsorily in accordance with the recommendations of the FATF. It involves the notification by the obligor to the competent central authority of the suspicion or suspicion that the funds subject to the transaction are related to laundering or terrorist financing.

Our Company aims to alert the competent authority (MASAK) about possible transactions for laundering proceeds of crime and financing of terrorism through suspicious transaction notification.

4.8.4. Suspicious Transactions Types

The suspicious transaction types, which have been published by MASAK and are set forth as enclosed to this document, are the suspicious transactions types that have been identified by MASAK. However; the suspicious transaction types set forth within should be considered not on the basis of a single criterion but also with respect to the provisions set forth herein in respect to knowing the customer. A transaction may, thus, be reported as a suspicious transaction even if it does not fit into any of the types set forth within the Appendix.

Such matters as those provided below constitute grounds for the reporting of a transaction as a suspicious transaction;

- Whether or not the customer is eager to provide personal information,
- If there is no apparent legal and economic purpose in place for the transaction, and
- Provision of misleading information, documents and contact details.

Although the types of suspicious transactions mentioned above serve as an important reference in identifying suspicious activities, the perception and experience of the individual conducting the transaction play a critical role in this process. Aware of this, our Company has identified enhancing the awareness of both its employees and representatives on this matter as one of its primary objectives.

In such cases, the transaction should be reported immediately and directly to the Compliance Officer via email. Verbal reporting is in contravention to the applicable procedure.

It shall be at the discretion of the Compliance Officer to decide whether or not to report any suspicious transaction reported thereto to MASAK. In the cases, where it is not considered by the Compliance Officer necessary to report to MASAK the reports filed by the departments, branches and the representation offices, the Compliance Officer shall issue such opinion thereof in writing in the form of a resolution and retain the same.

The involved parties and all concerned parties, who are knowledgeable about the reports, shall act with due care and in due diligence in accordance with the applicable legislations for the maintenance of the confidentiality and security of the suspicious transaction reports and the internal reports on the matter, which are filed within the organization of PayPorter, and for the protection of the involved parties.

4.9. Obligation to Provide Information and Documents

At PayPorter; any and all requirements in respect of the reporting activities to be carried out as a part of continuous provision of information and the provision fully and accurately of any information and documents, which the officials of the Financial Crimes Investigation Board, the Ministry of Finance of the Republic of Turkey and the other Auditors and Examiners provided within the applicable legislations may request, as well as any records associated to the same on any media and any and all details, information and passwords necessary for access to such records or for rendering such records readable, are and shall be fulfilled with the utmost care and in the utmost diligence.

4.9.1. Retention and Confidentiality of Information, Documents and Records

Any and all information, documents and records, which are required to be obtained and retained under the Act on the Prevention of the Proceeds of Crime, and the other applicable regulations in force, enacted on the basis of the said Act, shall be retained diligently for such periods and in accordance with such principles that are contemplated within the applicable legislations and in such manner that they are accessible when necessary. Any and all information and documents related to customer identification and transaction details shall be retained for period of 10 years from the date of the last transaction.

The scope of retention and submission obligation also encompasses the suspicious transaction reports and any attachments to the same.

4.10. Compliance Officer & Deputy Compliance Officer of the Company

PayPorter has appointed a compliance officer, who is in charge of and responsible for the development and monitoring of programs and strategies regarding the AML laws, rules, guidelines and regulations.

Compliance Officer;

Full Name	:	Ufuk SİNEL
Title	:	Compliance Officer
Phone	:	(+90) 212 275 41 01 - 313
E-mail	:	ufuk.sinel@payporter.com.tr
Address	:	Büyükdere Caddesi, Likör Yanı Sokak, AKABE Ticaret Merkezi No: 1 Kat: 3 Daire No: 13 Şişli/İstanbul

Deputy Compliance Officer;

Full Name	:	Eda ÖNER
Title	:	Deputy Compliance Officer
Phone	:	(+90) 212 275 41 01 / 331
E-mail	:	eda.oner@payporter.com.tr
Address	:	Büyükdere Caddesi, Likör Yanı Sokak, AKABE Ticaret Merkezi No: 1 Kat: 3 Daire No: 13 Şişli/İstanbul

5. DOCUMENTATION

- This policy shall enter into force on the date of its publication following its approval by the Board of Directors.

6. RECORDS

- The provisions of this policy are executed by the Board of Directors to which it reports.

7. REVISIONS

#	Date	Version	Prepared	Approved by	Explanation
1	17.06.2016	0	Compliance Officer	Board of Director	Date of entry into force of the Policy
2	22.05.2018	1	Compliance Officer	Board of Director	Annual revision
3	20.07.2020	2	Compliance Officer	Board of Director	Annual revision
4	25.06.2021	3	Compliance Officer	Board of Director	Annual revision
5	08.08.2022	4	Compliance Officer	Board of Director	Annual revision
6	13.04.2023	5	Compliance Officer	Board of Director	Annual revision
7	14.12.2023	6	Compliance Officer	Board of Director	Annual revision
8	01.03.2024	7	Compliance Officer	Board of Director	Annual revision
9	28.02.2025	8	Compliance Officer	Board of Director	Annual revision