AML POLICY

CONTENT:

I. Key Definitions

This section should include key definitions for basic terms used throughout the Manual as to allow all levels and types of staff to familiarize themselves with AML/CFT related matters.

"AMLCO/MLRO" means the Anti-Money Laundering Compliance Officer or Money Laundering Reporting Officer of the Company.

"AML/CFT" means Anti-Money Laundering and Combating the Financing of Terrorism.

"Board of Directors/Board/BoD" means the Board of Directors of the Company.

"Business relationship" means business, professional or commercial relationship between the customer and the Blueberry Payment Solutions Ltd ("**BPS**" or the "**Company**"), which is linked to the professional activities of BPS and that BPS expects, at the time of its establishment, to have certain duration.

"Customer" means a person that establishes a business relationship or performs an occasional transaction with the company.

"High-risk third country" means a third country, which is flagged by the European Commission under the provisions of paragraph (2) of Article 9 of the EU Directive by means of delegated powers and by FATF, and which has strategic deficiencies in its national AML/CFT regime thatpose significant threats to the financial system of the Union, and a third country which is classified by the Company as high risk, according to the risk assessment referred to in Article58a of the Law. List of High-risk third countries is provided in Annex No 4 to this Policy.

"PEP" means a Politically Exposed Person as defined in the AML Law.

"Senior Management" means an officer or employee of the Company with sufficient knowledge of the Company's money laundering and terrorist financing risk exposure and sufficient seniority to take decisions affecting its risk exposure and need not to be a member of the Board of Directors.

"Willful blindness" means the "deliberate avoidance of knowledge of the facts" or "purposeful indifference." It is the equivalent of actual knowledge of the illegal source of funds or of the intentions of a customer in a money laundering transaction.

"Structuring" means small transfers or small deposit amounts from customers that are trying to avoid recordkeeping requirements or trigger AML flag alerts from the any company (EMI).

"PEP" Means Politically Exposed Person.

Preamble

This Anti-Money-Laundering policy and Internal Control procedures and Standards (the "**AML Policy**") has been adopted by *Blueberry Payment Solutions* on a board level and applies to the company Blueberry payment solutions (acting as distributor on behalf of UAB "PAYRNET"). Strict compliance with this AML Policy is the responsibility of all Blueberry Payment Solutions employees.

II. Purpose

BPS is committed to the highest standards of anti-money laundering ("**AML**") and counter-terrorism financing ("**CTF**") compliance (collectively "**AML**") and requires management and employees to adhere to these standards to prevent the use of our services for money laundering purposes.

This AML Policy sets forth procedures for all transactions involving exchange of funds (electronically) with external parties and appropriate screening and monitoring requirements "know your customer" (KYC) policies (including the requirement to establish the identity of beneficial owners, in case of legal persons as customers,) record keeping requirements, the reporting of suspicious activities (STR/SAR) in accordance with relevant laws and training.

The standards set out in this AML Policy are the minimum requirements based on the Prevention and Suppression of Money Laundering Activities laws 2007 to 2018 the Lithuanian Law on the Prevention of Money Laundering and Terrorist Financing (the "**AML Law**"), and apply to the entire company for its operational activities and transactions.

The purpose of this AML Policy is to set the minimum standards and provide general guidance andclarity on BPS's effort to prevent and suppress money laundering terrorist financingand other illegal activities and to ensure compliance with all applicable legal and regulatory requirements.

III. BPS as distributor of PAYRNET

BPS is operating as an appointed distributor of UAB "PAYRNET" (further – **PAYRNET**), which is incorporated in Lithuania and authorised as an Electronic Money Institution in Lithuania and to this extent BPS must also follow and apply certain Lithuanian legal requirements, including those deriving from Lithuanian Law on the Prevention of Money Laundering and Terrorist Financing.

Due to distributor's status, BPS and its activities should be supervised and monitored by PAYRNET. This is required based on legal requirements applicable to PAYRNET the aim of which is to ensure the proper and compliant provision of licensed services through selected distribution channels (including appointed distributors) since from the regulatory point of view PAYRNET shall remain ultimately responsible for the compliance and legitimacy of appointed distributor's actions in relation to provision of such services on behalf of PAYRNET. Considering this, certain supervision and control measures might be applied by PAYRNET over BPS as distributor, including the following ones (the list should not be considered as exhaustive):

- MLRO of BPS shall be assigned to be responsible for the communication with PAYRNET and shall collect information on BPS's, as PAYRNET distributor's, activity, including number of customers serviced by BPS as an appointed distributor during the reporting time slot, profiles of such customers (e.g. types of customers, from what jurisdictions they are, to which risk groups they were assigned, number of customers with whom business relationship were terminated, etc.) in order to be able to report to PAYRNET, if so requested;
- Management of PAYRNET will always have a right to request information and / or documents related to activities of BPS, as PAYRNET's intermediary;
- PAYRNET will have a right to execute internal audit covering assessment of BPS's activities and its compliance with applicable AML / CTF requirements (to the extent related to BPS's services provided in its status as distributor of PAYRNET);
- PAYRNET will have a right to perform ad hoc audits over activities of BPS (to the extent related to its status as distributor of PAYRNET). For instance, to check few customers' files aiming to understand whether BPS complies with the legal requirements.

PAYRNET will acquaint BPS with its own AML / CTF procedures and all subsequent changes. BPS must ensure proper implementation PAYRNET's requirements in the AML / CTF area.

As from a regulatory point of view PAYRNET remains ultimately responsible for the provision of licensed services through BPS as distributor of PAYRNET, it is crucial for PAYRNET to ensure that activities of BPS are in line with applicable requirements. For this purpose, PAYRNET will share its own AML / CTF Policy with BPS prior to BPS starts providing services to customers as distributor of PAYRNET. BPS will have a duty to review the PAYRNET's AML / CTF Policy and tailor its own AML / CTF procedures so that they would be compliant with the ones applied by PAYRNET. As both AML Policies (of PAYRNET and BPS) are prepared inter alia based on Lithuanian legal requirements, they should match and not contradict each other in key areas.

IV. AML/CTF Procedures and controls

a. What is Money Laundering?

Money laundering involves taking criminal proceeds and disguising their illegal sources in order to use the funds to perform legal or illegal activities. **In other words,** money laundering is the process of making dirty money (derived/earned from illegal activities) look clean.

When criminal activity generates substantial profits, the individual involved must find a way to use the funds without drawing attention to the underlying activity or persons involved in generating such profits. Criminals achieve this goal by **disguising** the source of funds, **changing** the form or moving the money to a place where it is less likely to attract attention. Criminals' activities that lead to ML (i.e. predicated offences/crimes) can include: illegal arms sales, narcotics trafficking, contraband smuggling and other activities related to the organized crime, embezzlement, insider trading, bribery and computer fraud schemes, bribery and tax

evasion.

The United Nations 2000 Convention Against Transnational Organized Crime, also known as the "Palermo Convention" defines money laundering as:

- The conversion or transfer of property, **knowing** it is derived from a criminal offense, for the purpose of concealing or disguising its illicit origin or of assisting any person who is involved in the commission of the crime to evade the legal consequences of his or her actions.
- The concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of property **knowing** that it is derived from a criminal offence.
- The acquisition, possession or use of property **knowing** at the time of its receipt that it was derived from a criminal offense or from participation in a crime.

Money laundering often involves a complex series of transactions that are difficult to separate. However, it is common to think of money laundering as occurring in three stages.

Stage 1 Placement:
The physical disposal of cash or other assets derived from criminal activity. During this phase, the money launderer introduces the illicit proceeds into the financial system.

Stage 2 Layering:
The separation of illicit proceeds from their source by layers of financial transactions intended to conceal the origin of the proceeds. This second stage involves converting the proceeds of the crime into another form and creating complex layers of financial transactions to obfuscate the source and ownership of funds.

Stage 3 Integration:
The last stage of money laundering. Supplying apparent legitimacy to illicit wealth through the re-entry of the funds into the economy in what appears to be normal business or personal transactions. This stage entails using laundered proceeds in seemingly normal transactions to create the perception of legitimacy. The launderer, for instance, might choose to invest the funds in real estate, financial ventures or luxury assets. By the integration stage, it is exceedingly difficult to distinguish between legal and illegal wealth. This stage provides a launderer the opportunity to increase his wealth with the proceeds of crime.

Although money laundering is a distinctly different crime from the original underlying activity, BPS has chosen to put in place controls which makes its services unattractive to criminals of all kinds, irrespective of whether the activity taking place is considered to be money laundering.

Failure to adhere to the provisions of the AML Law - including those requiring customer due diligence, record keeping, ongoing monitoring, enhanced due diligence, reporting to the local FIU (Financial Intelligence Unit) can lead to significant **administrative penalties**.

Criminal penalties for money laundering include imprisonment for natural persons and restriction of business activities or liquidation of legal person (varies from a EU member state Jurisdiction to EU member state Jurisdiction but always within the lines of EU AMLD).

b. What is Terrorism?

After the terrorist attacks of September 11, 2001, the finance ministers of the Group of Seven (G-7) industrialized nations met on October 7, 2001, in Washington, D.C., and urged all nations to freeze the assets of known terrorists. Since then, many countries have committed themselves to helping disrupt terrorist assets by alerting financial institutions about persons and organizations that authorities determine are linked to terrorism.

Terrorism is the use, or threat, of action designed to influence government, or to intimidate any section of the public, or to advance a political, religious, or even ideological cause, where the action would involve violence, threats to health and safety, damage to property, or disruption of electronic systems.

The definition of "terrorist property" means that all dealings with funds, or property which are likely to be used for the purposes of terrorism, even if the funds are "clean" in origin is a terrorist financing offence.

Terrorist financing includes offenses related to:

- Fund-raising for the purposes of terrorism;
- Using, or possessing money for the purposes of terrorism;
- Involvement in funding arrangements;
- Money laundering – facilitating the retention, or control, of money which is destined for or is the proceeds of terrorism.

Although there are monitoring transaction controls, to avoid becoming conduits for terrorist financing the company employees must look at, among others, the following factors when reviewing the transaction history of an account:

a) Use of an account as a front for a person with suspected terrorist links.
b) Appearance of an accountholder's name on a list of suspected terrorists.
c) High volume of transactions in the account.
d) Lack of clear relationship between the e-money activity and the nature of the accountholder business or type.

Failure to adhere to the provisions of the AML Law – including those related to terrorist financing – can lead to monetary sanctions as well as it could be basis to invoke criminal liability.

c. Obligations

The issuer of the Blueberry prepaid MasterCard and voucher program is PAYRNET, a company incorporated in the Republic of Lithuania authorized by the Bank of Lithuania under the law
of Electronic Money and Electronic Money Institutions (license reference 72, issued on 28/08/2020) for the issuing of electronic money and provision of therelated payment

services . Blueberry Payment Solutions Limited acts as program manager for the

prepaid MasterCard
and voucher program (acting as an intermediary) and is responsible for the day-to-day operation and distribution of the program as agreed to by the Issuer.

The Blueberry program will be operating initially in Cyprus with services to be extended to Greece and other European markets in the future. It is BPS's responsibility andobligation to ensure that, where applicable, local host state AML/CFT laws are applied when providing services in the jurisdiction other than Cyprus under the distributor's status. Until BPS provides services only in Cyprus it must comply with the Cypriot National AML Law which is in line according to the requirements of the Directive (EU) 2015 /849 of the EuropeanParliament and
recently with the updated one Directive (EU) 2018/843. Lithuania specific requirements that may be imposed by PAYRNET must be also followed.

The services being provided are all operating on a cross-border (freedom to provide services) basis without the presence of a physical establishment by PAYRNET within the jurisdictions . Consideration has been given when drafting the procedures in this document to ensure that,
where applicable, local host state AML/CFT requirements have been met.

BPS, acting as distributor of PAYRNET, is required to apply AML requirement and should establish and maintain appropriate internal policies and internal control procedures relating to:

a) Customer and ultimate beneficial owner (UBO) due diligence;
b) Risk assessment and management;
c) Ongoing monitoring of Business relationship and/or operations;
d) Implementation of international sanctions and restrictive measures;
e) Keeping of logs;
f) Record keeping;
g) Renewal of customers and UBO identification and information;
h) Organization of training of employees with an aim to familiarize them with AML/CTF requirements;
i) Ensuring proper communication with PAYRNET in terms of provision of services under distributor's status;
j) Allocation of responsibilities in connection with implementation of AML/CTF requirements; and
k) Management and communication of information in connection with implementation of AML/CTF requirements.

V. Money Laundering Reporting Officer (MLRO)

The MLRO of BPS must be appointed and approved by the Board of Directors of the company as per the Appendix I.

The MLRO must act independently and autonomously to perform their duties and possess the appropriate seniority so as to command the necessary authority. The MLRO should have direct and timely access to any available information, records and documents which may be of assistance to him/her.

MLRO Duties and Responsibilities

Additionally, the MLRO of BPS is responsible for communicating with the compliance team of PAYRNET for all the AML matters as well as for the AML/CTF activities of BPS, monitoring the compliance with applicable legal requirements, including but not limited to:

- Ensuring timely and proper communication with and timely reporting to PAYRNET and, if so required, relevant authorities.
- Providing information to Senior Management PAYRNET about the operation and effectiveness of its policies, controls and procedures whenever appropriate and at least annually.
- Providing information, data and documents to PAYRNET in relation to customers' suspicious activity so that PAYRNET would be able to report to local FIU as required under applicable requirements.
- Developing, maintaining and updating a risk-based approach to AML/CTF.
- Identifying any situations of highest risk of ML/TF.
- Prepare an annual business wide risk assessment and present it to Senior Management and PAYRNET.
- Ensuring implementation of transaction monitoring procedures.
- Maintaining a record of its policies, controls and procedures, risk assessment and risk management including the application of such policies and procedures.
- Applying measures to ensure that its policies, controls and procedures are taken into account in all relevant functions including in the development of new products, dealing with new customers and in changes to business activities.
- Ensuring that AML/CTF policies and procedures are adapted to regulatory changes and standards in a timely manner.
- Ensuring that AML/CFT policies and procedures are revised and updated on a regular basis (at least annually).
- Ensuring that all required records and logs are kept within BPS.
- Organizing and ensuring ongoing employee education in AML/CTF area including training related to identification of suspicious activity, customer identification, record keeping.
- Ensuring that all employees are familiar with AML/CFT policies and procedures and with all specific requirements that are applied by PAYRNET and must be ensured within activities of BPS as PAYRNET's distributor.
- Formulate BPS's AML strategy, covering the policies and procedures, technology, system resources, and risk analyses.
- Implement the AML policies and procedures within BPS and ensure the compliance by the relevant departments.
- Provide sufficient and objective information about the effectiveness of money laundering controls and measures to the Board of Directors and Senior Management.
- Ensuring that the following information is stored securely and electronically and will be made available to PAYRNET when appropriate:

- Customer identification file
- Customer information collected throughout the Business relationship/or the onboarding process.
- Information on customers' monetary operations or transactions
- SARs and their material
- MLRO internal reports (if applicable)
- Training information (AML matters)
- Other necessary information

- Keeping an internal SAR log for record keeping and such files should have limited access – to only relevant individuals within the company for security purposes.
- In case of an investigation of SAR/STR the investigation should be undertaken by the MLRO who must record the results of the investigation against the customer file and keepthe records in a confidential place (hard copy or soft copy), by informing PAYRNET 's MLRO, and be able to provide all such data to the MLRO of PAYRNET upon request.
- In case the MLRO is discovered to have failed to report a transaction which knew to be suspicious or to have involved in money laundering, will be potentially liable under applicable laws unless there is a good reason for not reporting the transaction to the issuer.

Worth mentioning that certain AML/CTF tasks may be delegated by the MLRO, however the ultimate responsibility resides with the MLRO of BPS.

VI. Duties and responsibilities of Senior Management and Board of Directors

Embedding a culture of compliance into the overall structure of BPS is critical to the development and ongoing administration of an effective AML/CFT program. As per the national law the ultimate responsibility for the AML/CFT compliance program rests with BPS's Board of Directors. Hence, the Board of Directors and Senior Management must set the tone from the top by openly voicing their commitment to the AML/CFT program, ensuring that their commitmentflows through all service areas and lines of business, and holding responsible partiesaccountable for compliance. For these reasons, below are their key responsibilities as it concerns the AML matters of BPS:

- Responsible AML Director (member of Board of Directors)
- Appointment of the MLRO
- Establishment of the risk appetite and Customer Acceptance Policy (CAP)
- Ensure the update of CAP
- Approval of policies, procedures and controls
- Measures to identify the need for adjustment of procedures
- Enhancement of adjustment of procedures, where needed
- Approval of establishment or continuation of a BR with PEPS or high risk customers
- Provision of appropriate and adequate training to the Board of Directors, Senior Management and staff.

VII. Risk appetite statement

BPS has zero tolerance for financial crime, regulatory breaches, and any attempt to circumvent the company's financial policies and controls. BPS also has zero tolerance toward the facilitation of financial crime, ML/TF and fraud.

Consequently, BPS adheres to the following core principles which are also being shared with its card issuer PAYRNET:

- To avoid knowingly conducting business with persons believed to be engaged in an unlawful behaviour;
- To avoid risks that could jeopardize strategic plans, reputation, or reputation withregulators;
- To avoid or cease any activity where the company's internal control mechanisms would not be sufficient to protect from risks that exceed the tolerance threshold;
- To dedicate a competent MLRO, who is liable to properly manage, supervise andimplement ML/TF prevention measures;
- To ensure proper testing;
- To regularly perform business wide risk assessment aiming to identify changes with customers, products, geographies, and distribution channels and verify whether existing control measures are sufficient to moderate the residual risk.

Lastly, the **Customer Acceptance Policy (CAP)** is fundamental to any effective AML program and reflects the firm's risk appetite. For this reason, BPS has to be clear and loud on which basis might reject or terminate an existing BR with a customer which is outside the risk appetite of the company through its customer acceptance policy **(Annex II).**

VIII. Risk based approach

a. Business Wide Risk Assessment

In order to adopt a risk-based approach AML/CFT program, BPS shall conduct an AML business wide risk assessment at least once every year to **identify and assess** the high-risk areas related to AML/CFT, i.e. BWRA (AML oriented).

Business wide risk assessment should be also performed prior to the launch of any product, business practicesor the use of new developing technologies or any other significant change might occur.

The risk factors below shall be considered in the business wide risk assessment:

1. Products and services risk factor.
2. Customer Risk factor.
3. Countries and Geographical risk factor.
4. Delivery Channels.

The AML business wide risk assessment must be presented to the Board of Directors and approved. BPS's business wide risk assessment should be also presented to PAYRNET upon its request.

b. Customer risk assessment

Following the risk-based approach that BPS should adhere to, a risk assessment should be conducted for each customer at the point of onboarding process and on ongoing basis as well. Each customer shall always be assigned to a relevant risk group (low risk, medium risk, high risk, unacceptable risk). When a risk is flagged then BPS should take action to mitigate the risk highlighted or conduct additional monitoring and reporting to control those risks.

To this extent, BPS has adopted the use of a customer risk assessment taking into consideration the following risk factors:

1. **Country Risk**: Country of registration, residence, address, trading and registered country of UBO address, country of business operating. In more detailed analysis:
   a. Country of origin (nationality) – a customer coming from a jurisdiction with lower standards of legislation and/or measures against ML or TF, less developed legal or judicial systems or with unstable political environment may pose high risk;
   b. Country of residence – the jurisdiction(s) in which the customer is based (residential address).
2. **Customer Risk:** Natural person, or legal entity, regulated or not, specific structure (SME,limited liability, micro-enterprise), ownership structure (low, medium, high).
   a. Business and profession – customer's business or professional activity in whatever country they are associated with.
   b. Reputation – customer's reputation in whatever country they are associated with (e.g. adverse media through open source internet search).
   c. Nature and behaviour – a customer's nature and behaviour in whatever country they are associated with.
3. **Products and Services risk:** nature of business, financial services used (payday loans, card only account, wealth management, invoice management, remittance, etc.):
   a. Transaction value or history - when the customer is conducting transactions through his products and services he is using that are not proportionate with his business and profession or source of wealth that has provided to us during the onboarding/CDD process.
4. **Delivery Channels:** new technologies/devices used to provide services, promoted from an already existing merchant through Marketing tools.

In case the customer is identified of holding a prominent public function being a Politically ExposedPerson (PEP) or being immediate family member or closely associated (1st degree), as defined below in section VIII, are being directly graded as high risk customer and EDD is being implemented and approval from the MLRO is being obtained prior to the establishment of a Business relationship. A more detailedanalysis for the directly high-risk customers can be found in the **Annex II** (Customer Acceptance Policy) of this document.

Depending on the particular risk group to which each customer is assigned, BPS is tailoring measures for CDD and monitoring (e.g. if a customer is flagged as high risk customers, EDD is applied and if a customer is of low or medium risk then CDD is performed.). To mitigate its residual

AML/CTF risk BPS is not using Simplified Due Diligence process for any of its customers, either potentials or already existing ones.

IX. PEPS

A politically exposed person (PEP) is defined as an individual who is or has been entrusted with a prominent public function either in the republic of Cyprus (Domestic PEPS), Lithuania, other EU member states andinternational or foreign state institutions (Foreign PEPS). PEPs are deemed to pose a higher money laundering risk as their position may make them vulnerable to corruption. MLRO of BPS has to advise front line employees of the company on a case-by-case basis what additional measures should be taken in respect of this category of customer, while all accounts that are PEP related (UBO of a company, or private individual account) must be approved bythe MLRO and EDD to be implemented.

Prominent Public Functions according to the guidance provided from UAB "PayrNet" are the following:

(a) The Head of the State, the Head of the Government, a minister, a vice-minister or a deputy minister, the State Secretary, the Chancellor of the Parliament or the Government or a ministry.
(b) A member of Parliament;
(c) A member of Supreme Courts, the Constitutional Courts or any other supreme judicial authorities whose decisions are not subject to appeal;
(d) The mayor of a municipality, the head of a municipal administration;
(e) A member of the management body of the supreme national audit and control body of the chairman, deputy chairman, or member of the board of a central bank;
(f) An ambassador, a chargé d'aaires ad interim, Commander of Cyprus Armed forces, Commander of the Armed Forces and Units, Chief of Defence Unit or a high-ranking officer of the foreign armed forces;
(g) A member of a managing or supervisory body of a state-owned entity, public limited liability company, private limited liability company where the state owns shares or a proportion of shares amounting to more than ½ of all votes at a general meeting of shareholders of said entities or companies and which are considered as large companies under the Law on Financial Statements of Undertakings of the Republic of Cyprus or any other state;
(h) The head or deputy head or member of a managing or supervisory body of an international intergovernmental organization;
(i) The head, deputy head, or member of a managing body of a political party.

The list of prominent public functions may vary from time to time.

The term PEP shall also include immediate family members (spouse or partner, children or their spouses and partners, and parents and parents-in-law, siblings), and close associates that are reputedly known as (1) a natural person who, together with a person who performs or has performed prominent public functions, is the participant of the same legal entity or the organisation without the status of legal entity or maintains other business relations; or (2) a natural person who is the only beneficial owner of a legal entity or an organisation without the status of legal entity that is established or operating de facto with a view to receive economic gain or other personal benefits for a person who performs or performed prominent

public functions.

PEPS identification

BPS has established internal controls and procedures when employees are identifying any customers who are PEP or immediate family members to PEPs or close associates during the onboarding process and prior to the establishment of Business relationship with them. A senior management approval is required to be obtained for all PEPs that are willing to enter into Business relationship with BPS or who become PEP in the course of Business relationship while an EDD should be established containing at minimumthe following information in the file:

- Full scope of information, data and documents as in case of CDD;
- Information and evidence of source of funds and source of wealth;
- The research front line employees and MLRO have undertaken as a part of their decision-making process to submit this account for approval to the MLRO (or denial);
- The approval notice from the card issuer PAYRNET to enter into the Business relationship (if so required by PAYRNET); and
- Copies of ongoing enhanced transaction monitoring and reports of MLRO findings (if applicable).

Use of Lexis Nexis

Except the open source ("Google Searching") for the customers, BPS is using Lexis Nexis a screening tool program from Thomson Reuters company. Lexis Nexis/World Compliance is an internet based-risk screening service tool which enabling users of BPS (front line employees and MLRO) to instantly check individuals or entity names against a worldwide data set (sanctions from UN, OFAC, EU, targeted sanctions, Interpol Data set, worldwide adverse media set, worldwide data of PEPS and close associates etc.). Updated in real-time its quick search functionalities allow the employees of the company to identify any potential risks the person, entity or their associates may hold.

Lexis Nexis screening tool account contains 20+ different fields ranging from identification fields like Name, Last Name, Aliases, Nationality and Date of Birth to more risk specific information such as official lists, PEP categorization, a synopsis offering a concise summary of the information found and lists of companies and associates reported to be linked to the profiled entity in question.

Front line employees are required to conduct a Lexis Nexis screening prior to the completion of opening any account.

The circumstances below should always be escalated to the MLRO of BPS prior to the acceptance (or denial) of the customer and entering with the customer into Business relationship.

(a) If the customer is identified under a category or subcategory of terrorist, or appears on the OFAC's Specially Designated Nationals and Blocked Persons List or the EU's list ofsanctioned individuals, the relevant customer service employee should escalate the customer's file to the MLRO for consideration of submitting an STR to the relevant authorities.

(b) If the customer is identified under a category or subcategory of PEP or comes from a country covered in the list of high-risk countries maintained by PayrNet including

any other high risk countries according to BASEL index or Non-Cooperative Countries published by FATF on Money Laundering ("FATF blacklist").

Simply put, through Lexis Nexis/World Compliance Blueberry perform KYC investigations on our business partners and cardholders in order to better understand whether there could be possibility of them being involved in any money laundering, terrorism financing activities, forgery, fraud, and human/drug trafficking and other related offences. **Sanctioned persons cannot be onboarded by BPS while PEPs may be onboarded but they must be always assigned to high-risk customers group category and EDD measures should be applied towards them.**

X. KYC/B minimum requirements during the onboarding process (CDD /EDD)

Identification of the customer (natural persons /private individual) always means identification of the natural person and their representatives (if any). Identification of the customer (legal person /entity) always means identification of the customer , its representatives and UBO (above 25% or having other control; for high risk customers – 10 % threshold is applied). Additionally , BPS should collect the information necessary to understand the purpose and intended nature of customer's relationship with the company. BPS is following the guidance that has been provided from is card issuer PAYRNET for verifying, identifyingand assessing the level of risks posed from their customers (Annex III-KYB/C PAYRNET Guidance).

Customer Due Diligence

BPS must apply customer due diligence measures for its customers in the following

situations: a) Prior to establishing Business relationship with the customer;
b) When BPS suspects money laundering or terrorist financing;
c) When BPS has doubts towards the veracity or adequacy of documents or information previously obtained forthe purpose of identification or verification;
d) When BPS becomes aware that the circumstances relevant to an existingcustomer risk assessment scoring have changed.

In case BPS is unable to apply CDD measures on a customer then BPS should not proceed with any execution of transactions for the customer , not establish Business relationship with the customer or end an existing Business relationship with the customer, if applicable (and consideration for SAR from the MLRO to PAYRNET).

<u>Necessary information</u>

The below information should be obtained from the customer during the CDD process:

- Information of the intended turnover and scale of the business which the customer intends to transact with BPS;
- Information on the expected currencies and destination of the payments;
- Details of the business, its products and services;
- Details of the products and services the customer will use with BPS;
- PEP status of the customer (its representative, key director, UBO);
- Purpose of the account;

- Nationality;
- Date and country of birth (personal code, if available);
- Occupation;
- Employer's Name;
- Contact number (mobile phone);
- E-mail Address;
- Source of funds;
- Other required information.

Having in mind that the customer should confirm the accuracy and validity of the above information and BPS should verify it.

Natural Persons (private individuals)/KYC necessary documentation

The following documentation is requested and must be provided by the customers during the identification process in order for key information be verified:

- A photo of a valid ID document* (back and front end)
- Selfie of the customer holding his/her ID or a real time video showing his/her ID and his/her face
- Current residential address (no older than 3 months)
- Source of funds or source of wealth (upon request)

* Identification Document refers to any of the following: Passports, National ID cards, EEA issued Drivers Licenses.For Cyprus citizens: a Cypriot residency permit should always be obtained in addition.

The above information and documents are to be received during remote identification – through real time photo (video) transmission.

Legal Persons

Representative of the legal person must go through the same process as natural person, i.e. representative should participate in real time photo (video) transmission session where s/he provides his/her ID document photo and facial image (selfie) either as real time photos or videos.

In addition, in case of legal persons (legal entity), BPS shall verify the legal existence and corporate structure of such corporate customer, as well as the authority and identification of all persons purporting to act on their behalf. BPS shall obtain:

- Incorporation documents such as Articles of Incorporation or by-laws (notarized and apostilled); and
- Extract from the relevant Companies Register (notarized and apostilled);
- Documents proving official or principal business address; and
- Documents proving list of directors (notarized and apostilled); and
- Documents proving principal stockholders owning at least twenty five percent (25%) of the capital stock, contactnumbers, and beneficial owners; and
- Documents proving sources of funds and wealth (e.g. financial statements).

The Company does not rely on the customer due diligence performed by third parties or introducers.

XI. Enhanced Due Diligence (EDD)

For High risk flagged customers (according to their risk scoring assessment) BPS will conduct an EDD as per its Policies and procedures and the business wide risk assessment feedback. The steps that are taken to carry out an EDD should vary depending on the specific circumstances and customer type.

Apart from other cases when high-risk customer is established and EDD are applied, EDD must be always applied in the following cases:

(a) With regard to business relations or transactions with customers established / residing in high-risk third countries (Annex No. 4 to this Policy), the following increased customer due diligence measures shallapply:
   a. collection of additional information on the customer and the beneficial owner;
   b. collecting additional information on the planned nature of the business relationship;
   c. collecting information and documents on the origin of the funds and the source of the wealth of the customer and beneficial owner;
   d. collecting information on the purpose of transactions planned or executed;
   e. obtaining approval from Senior Management to establish or maintain a business relationship with such a person;
   f. requesting the customer to make the first payment from his/her/its bank account opened with EEA credit institution;
   g. carrying out increased and continuous monitoring of this business relationship.

(b) In transactions or business relationships with a PEP:
   a. obtaining approval from Senior Management to establish or maintain Business relationship with such a person;
   b. collection of additional information on the customer and the beneficial owner;
   c. collecting additional information on the planned nature of the business relationship;
   d. collecting information and documents on the origin of the funds and the source of the wealth of the customer and beneficial owner;
   e. carrying out increased and continuous monitoring of this business relationship.

XII. Transaction monitoring

BPS understands the importance of monitoring and a need to identify any suspicious transactions that are related with its customers (either for fraudulent reasons, money laundering or terrorist financing).

The ledgers of BPS are passing through compliance AML firewalls as instructed from our card issuer PAYRNET.

XIII. Suspicious Activity Report (SAR)

Suspicious Activity is considered:

- any suspected violation of laws or regulations;

- a suspected transaction related to money laundering or to terrorist financing;
- a transaction that appears to have no legitimate or reasonable business purpose;
- a payment or transaction which is suspected to be related with property that is directly or indirectly received from illegal activity or while participating in such illegal activity and/or is suspected to be related with terrorist financing.

How to Identify (Red Flags):

- Customer is reluctant to provide information when opening an Account or gives false information.
- Several unrelated customers with the same address.
- Customer who will give only a P.O. Box mail address.
- Customer who pays with numerous methods all with a face value under €10,000.
  Customer wants payment made in an unusual manner to unrelated business or person.
- No cardholder authorization involved in the transactions.
- Fraudulent processing of transactions, processor needs to be investigated/reported.
- Questionable merchant activity.
- At the time of entering into a Business relationship, the customer (representative) is reluctant to provide information necessary to identify the customer, provides documents which raise doubts as to their genuineness, authenticity, etc.
- It is difficult to obtain from the customer information or documents necessary for the monitoring of the Business relationship: it is difficult to contact the customer, customer's place of residence / registration as well as contact details often change; nobody answers the phone number provided by the customer or representative or it is always disconnected; the customer or representative fails to respond when addressed via e-mail.
- The customer is unable to answer questions regarding ongoing / planned financial activity and the nature thereof, is excessively nervous.
- The customer expresses a wish to close the bank account when asked to provide the information necessary for monitoring of its Business relationship.
- The monetary operations or transactions of the customer are not in line with the types of activities indicated by the customer during customer's identification process.
- The nature of the monetary operations or transactions that are being conducted by the customer raise a suspicion that the customer is seeking to avoid the entering of the monetary operations and transactions into the registration logs maintained by BPS.
- The flow of goods and settlements made for them do not match: companies or individuals unrelated to the transaction pay for the goods.
- The customer carries out a transaction and makes a payment (payments) which is beyond the customer's possibilities known to BPS or requires to make an advance payment or another payment exceeding the regular amount.
- The customer or the owner of the property requests to pay the amount belonging to the customer to persons who are clearly unrelated to customer's normal activity.
- The whole advance payment, other payment (or a major part thereof) is made on the customer's behalf by persons who are clearly unrelated to customer's normal activity.
- The customer is continuously engaged in transactions in property the value whereof is clearly not in line with the average market value.
- The customer carries out monetary operations or concludes transactions without any apparent economic justification.
- The customer, representative or the person on behalf of whom the monetary operation or transaction is being carried out, is subject to financial sanctions.
- The age, current position, financial status of the customer are objectively not in line with the financial activity conducted by this customer (e.g. the customer's income is small compared to the scope of his / her financial activity).

- The customer does not perform monetary transfers to its account opened at the EU member state, in which the customer is registered, or the amount of funds transferred to the customer's account opened at the state of registration thereof constitutes a negligible part of all the monetary operations carried out in BPS over a year or the amounts of funds kept in it.
- Monetary operations or transactions are carried out with natural and legal persons located in high-risk regions (e.g. with countries which are not members of the FATF or do not have observer status with the FATF and are not members of the international organization combating the ML / TF; with countries where terrorist organizations are active), whereas the economic justification of the monetary operations or transactions is unclear.
- The customer permanently resides in a country which is not a member of the FATF or does not have observer status with the FATF and is not a member of the international organization combating the ML / TF, whereas the economic justification of the monetary operations or transactions carried out by the customer is unclear.
- The customer constantly performs monetary operations or concludes transactions with legal entities or other organisations, registered in the target areas.
- Chip/PIN Failures.
- Counterfeit transactions.
- Transactions from lost, stolen or not received cards and counterfeit cards.

Once a transaction has been identified as suspicious, the employee must:

The employee should report the incident to the MLRO of BPS and wait for instructions.

Employee must keep the original records of the transaction and deliver them to the MLRO of BPS.

XIV. Reporting requirements

PAYRNET based on the AML/CTF manual and other applicable requirements, remains **responsible and fully liable** for the reporting to FCIS (Lithuania F.I.U.).

Having in mind that BPS does not have separate reporting duty to FCIS, the MLRO of BPS is obliged to raise an internal Suspicious Activity Report immediately to PAYRNET (within the shortest term possible) if he/she considers that there is knowledge, suspicion, or reasonable grounds for knowledge or suspicion that another person is engaged in ML/TF. By executing such (internal) report the MLRO, or Director or employee concerned will have met his obligations under the policy as well as its legal obligations.

An internal SAR template exist for this purpose. In case of a submission of such report the following process occurs.

- The internal SAR should be uploaded to the secure drive folder that is shared between BPS and PAYRNET accompanied with the KYC pack of the suspect/end user for PAYRNET review and consideration.
- Once the internal SAR is uploaded to the shared folder, BPS should send an e-mail to compliance@railsbank.com in order to notify PAYRNET that a new SAR has been created.
- Upon receiving the internal SAR from the company, PAYRNET sends a "receipt" including a reminder with regard to tipping off.

As also mentioned in the Duties and Responsibilities of this document, in case the MLRO of BPS fails to report a transaction which knew to be suspicious or to have involved money laundering will be potentially liable under applicable laws unless they have a good reason for not reporting the transaction to the issuer.

XV. Record Keeping

Record Keeping. Logs. Data Storage

BPS as well as its card issuer PAYRNET have a legal obligation to keep logs which contain specific and detailed information established under the AML Law.

Consequently, BPS should keep at least the following logs:

a) Log of suspicious activity and reports submitted to its card issuer PAYRNET.
b) Log of monetary operations and transactions exceeding Euro 15,000 (cash or through outward/inward transfers).
c) Log of customers with whom transactions or the Business relationship have been terminated due to circumstances related to infringements of the procedure for the prevention of ML/TF, including cases when Business relationship was terminated because customers tried to conceal information about themselves or UBOs, did not provide all required documentation etc.

Forms of logs are provided in Annex No 6 to this Policy.

Data is entered in the logs in chronological order, on the basis of the documents supporting the monetary operation or transaction or other documents with legal extracts related to performance of the monetary operations or conclusion (or termination) of transactions, or termination of the business relationship, immediately but no later than within three business days as of the performance of the monetary operation or conclusion of transaction, or the date when the specified circumstances occurred or were established.

Logs may be kept in a paper or electronic form / in the system.

BPS follows the AML/CTF Manual for record keeping that has been provided from PAYRNET. This is to ensure that all decisions made during the lifecycle of a customer's Business relationship are documented to show that a risk-appropriate level of CDD and ongoing monitoring was carried out by the company.

The MLRO of BPS will ensure that the following information is stored securely and electronically and will be made available to PAYRNET when requested.

- Customer identification information.
- Customer information collected throughout the Business relationship.
- Information on customer's monetary operations or transactions.
- SARs and their material.
- MLRO internal reports.
- Training information.
- Other necessary information.

BPS shares the same time frames on record keeping as per the table below which is in line with the guidance provided from its card issuer:

Type of data	Timeframe
Data of the logs	8 years as of the day of the end of the Business relationship with the customer
Copies of customer's (representative's) ID documents, identity data of UBOs, identity data of funds beneficiaries, records of real-time video identification or real-time photo transmission made during remote identification, other data received during the customers' identification, agreements and invoices collected in relation to the Business relationship with the customer (in cases of several products where one product is terminated, nonetheless all the information relating to the customer must be stored for 8 years from the day of the last product termination)	
Documents and data confirming performance of the monetary operation or transaction	8 years as of the date of performance of the monetary operation / transaction
Correspondence with the customer related to the business relationship and AML/CTF matters (both official correspondence with the customer and also correspondence by emails, via internet banking tool and correspondence by other electronic means)	5 years as of the day of the end of the business relationship with the customer
Letters and documents by which findings of the investigation of complicated or unusually large transactions and unusual structures of transactions are documented	5 years
AML training material	5 years
The time limits for record keeping may be additionally extended for no longer than two years upon a reasoned instruction of a competent authority	

XVI. Training

Training must be provided to all employees who have access to or deal with customers of BPS. Key components of the training should be as follow:

- Identifying PEPs within the customers' base.
- How to identify Suspicious Activities (red Flags) and that the funds received from a PEP do not derive from a corrupt source.
- Record keeping and reporting requirements.
- Verifying customer identification.

Employees are required to understand and comply with the contents of the AML Program and sign an acknowledgement declaration form that will be retained in their personnel file or with the AML files.

Existing employees who have access to card holder's accounts and or deal with BPS customers, will receive annual refresher AML training that will be documented and retained in their personnel file or with the AML files.

Training must be held at least once per year (more often to employees whose functions are closely related to AML area).

XVII. International sanctions

All the time it should be checked whether customers or their UBOs (if any) or representatives (if any) are not listed in lists in relation to which international financial sanctions are imposed. Such lists should be checked:

- Before entering into the Business relationship with the customer by making search in the compliance database used for financial sanctions application, PEPs status and negative media search; and
- On a regular basis during the Business relationship period which is ensured by automatic daily screening of the whole customers' database within the compliance database.

If relevant, BPS shall also ensure that check against application of international sanctions is performed against the recipients (payees) of funds indicated by the customer in payment transfers.

BPS shall not conduct business with customers who themselves, their representatives (if any), UBOs (if any) and directors (if any) are imposed with international financial sanctions of the UNO, European Commission and/or OFAC. The updated version of the Consolidated List is available on (not all provide possibility to search for free):

- The website of the United Nations Organization ("UNO") at: LINK
- Website of the European Commission ("EU") at: LINK
- The website of the Office of Foreign Assets Control ("OFAC") at: LINK

The MLRO of BPS shall periodically follow information published by the Ministry of Foreign Affairs of the Republic of Lithuania regarding entry into force of international sanctions. Relevant information provided at: LINK

If during the performance of the customers' identification process or during the Business relationship with the customer it is identified that the customer, its representative (if any), director (if any), UBO (if any) appears to be on the list, the employee of BPS who identified this shall immediately notify about this the MLRO of BPS. In this case the following actions should be performed:

- The MLRO of BPS should immediately (not longer than within three (3) business hours) inform the Chief Executive Officer of BPS and PAYRNET about such finding;
- PAYRNET shall take relevant actions aiming to prevent from servicing customers subject to financial sanctions following internal procedures of PAYRNET and applicable legal acts.

XVIII. Client Exit Policy

The Company assesses all existing and prospective Clients on a proportionate, objective and non-discriminatory basis. When carrying out an assessment, the Company takes into account applicable laws and regulations, internal policies and ensures legal and regulatory protection of its Clients and staff.

Business Relationship with the Client may be terminated (provision of services to a Client may be ceased) on the following basis:

- The Client wishes to terminate Business Relationship on his/her/its own initiative;
- Client's payment account is closed due to inactivity;
- Business Relationship are terminated on the Company's initiative or where so required by legal acts.

a) Termination of Business Relationship based on Client's initiative

The Client has a right to terminate Business Relationship with the Company without specifying any reason and unilaterally without applying to court by notifying the Company of the termination no later than 30 (thirty) calendar days (unless other term is agreed with the Client separately) in advance of its termination to the Company's e-mail address: [help@blueberry.com].

b) Account closing due to Client's inactivity

If the Client has an account opened with the Company and has not logged in or used the account via mobile application or website or in any other way did not perform any actions in the account for more than 1 (one) year, the Company will deem the account inactive.

If the account is deemed inactive, the Company shall send the Client via e-mail a notice regarding inactive account and ask the Client whether he/she/it wants to close it or continue to use it. The notice should include:

- Information that the account is deemed inactive;
- Applicable commission fees for further account maintenance;
- Information that if the account still has a positive balance and the Client will not close the account, the applicable commission fees will be further applied and deducted from the account balance until the Client closes the account or until the account balance reaches 0 (zero) Eur which will be also the basis to close the empty account for the Company;
- A right of the Client to close the account and, if there are funds in the account, a right of the Client to transfer funds left therein to his/her/its other payment account.
- Further actions of the Company to be taken (i.e., from the ones indicated in clauses When account has 0 (zero) balance and When the account has positive balance below).

- When account has 0 (zero) balance:

The Company has the right to terminate Business Relationship with the Client as well as to close Client's account only after 60 (sixty) calendar days (unless other term is agreed with the Client separately) pass from the notice submission to the Client, as indicated in above item.

The Client must be notified about the closed account in accordance with above paragraph immediately thereafter.

- When the account has positive balance:

If Client's account has a positive balance, the Company by the written notice referred to in item re (ii) Account closing due to Client's inactivity (above) must also inform the Client that the Company will continue applying commission fees for maintenance of the inactive account which will be deducted from the account balance until (a) the Client will close the account and will take back the remaining funds which will form the basis for the Company to close the account; or (b) until the account balance become 0 (zero) Eur and then the Company will close the account automatically.

If the account balance is high and it does not become 0 (zero) after 1 (one) year of account inactivity during which the Company applied commission fees as was indicated to the Client in the notice, the Company after such 1 (one) year passes must again submit a notification to the Client informing him about the remaining account balance and further deduction of the commission from the account balance if the Client will not express his/her/its wish to close the account and take back the funds.

The Client must be notified of the closed account in accordance with above paragraphs immediately thereafter.

ANNEXES

The following list of documents are an integral part of this Policy:

Annex No 1 – Approval of MLRO (minutes of meeting).
Annex No 2 – Customer acceptance Policy.
Annex No 3 – KYB/C PAYRNET guidance to customers (minimum CDD requirements).
Annex No 4 – High risk and prohibited countries list.
Annex No 5 – Acceptable evidence of sources of wealth and funds.
Annex No 6 – Forms of Logs.

Annex I (Approval of MLRO)

Blueberry Payment Solutions or "the Company"

Minutes of Meeting of the Board of Directors held on 06 January 2021 at 20 Charalambou Mouskou Street, ABC Business Centre, 5th Floor Office 504, Paphos 8010, Cyprus in accordance with the company's Articles of Association

---

Directors Present:
Panagiotis Andreas Christofides (CEO)

Presenters and Attendees (SM):
Rhyan Austin Bridle (CTO)
Mario Peter Christofides (Head of Business Development/COO)
Pambos Neoptolemou (Senior Compliance Officer/MLRO)

Company Secretary:
Marios Peter Christofides

1. Agenda Meeting Convened

The CEO of the company opened the meeting at 14:00 and welcomed the members of the meeting and the new member of the company Pampos Neoptolemou with the position MLRO.

CEO advised the members of the meeting that according to EU AMLD and our national legislation (Cyprus as member state of EU), a Director of the company has to be appointed to act on behalf of the company for AML matters (i.e., a responsible AML Director has to be in place). Taking this into consideration the Board affirmed the appointment of Mr. Panagiotis Christofides for this role with effect of 06/01/2021. According to the 4th AML Directive and the national law the MLRO of the company has to be also approved from the BOD and today is being approved.

The duties and responsibilities of the AML responsible director and the new MLRO of the company have been presented and explained in the meeting.

Resolution of the meeting on a board level

a) Approve and adopt the AML responsible Director duties.
b) Approve the new MLRO of the company.

c) Approve the new duties and responsibilities of the MLRO of the company (as per the AML policy of the company).
d) Requested from the MLRO of the company to draft a BWRA (AML oriented).

Appendix 1 (Notes presented to the Board & SM)

Appointment of the AML responsible Director

Background and purpose

2. Article 58D of the Prevention and Suppression of Money Laundering Activities Laws of2007 and 2019 ("the Law") requires the appointment of a competent member of the Boardof Directors ("Responsible Director") to be personally responsible for the implementation of the provisions of the Law and other relevant policies related with our sponsor EMD (UABPayrNet) and or circulars and/or regulations, including any relevant acts, Directives and Regulations of the European Union.

3. This document outline BPS's approach to ensure compliance with Article 58D of the national law and the (4th and 5th AMLD).

Appointment of a Responsible Director

4. The appointment of the AML responsible Directors is effected from 07/01/2021.

Competency of the Responsible Director

5. The responsible Director must be a member of the Board.
6. The responsible Director must have experience, in the business judgment of the Board that would be helpful in executing the duties and responsibilities delegated to the position.

Duties and Responsibilities of the Responsible Director

7. The duties and responsibilities of the Responsible Director shall include each of the items enumerated in this section and such other matters as may, from time to time, be required under relevant laws or delegated by the Board.

   (a) *Implementation of the law*- The responsible Director is **personally** responsible for the implementation of the provisions of the Law and any relevant AML/CFT Directives and/or circulars and/or regulations, including any relevant acts, Directives and Regulations of the European Union or which should also be inline with the Policies and procedures of our Distributor. The Responsible Director will also ensure the Board of

Directors and Senior Management are informed of their responsibilities under the Law and other regulations and any changes or developments thereto.

(b) *Supervision of the MLRO of the Company* – The responsible Director shall be responsible for the supervision of the MLRO.

(c) *AML Business Wide Risk Assessment (*AML Risks)- The Responsible Director shall be responsible for the effectiveness of the Company's AML risk management arrangements. The Responsible Director shall review the AML Business Wide Risk Assessment on an annual basis, or more frequently as required, and recommend to the Board for approval.

(d) *AML Policy* – The Responsible Director shall be responsible to review and approve the Company's AML Policy and any significant changes related thereto. CEO shall also oversee that the AML Policy is effectively communicated to all employees that manage, monitor or control the customers' transactions with responsibility for the application of the practices, measures and procedures determined.

Relationship between the Responsible Director and MLRO

8. Whilst the MLRO may have other reporting lines for day-to-day operational purposes the Responsible Director has **overall accountability** for the supervision of the MLRO in order to ensure that the MLRO fulfils all requirements outlined in the AML policy of the company.
9. The MLRO has direct access to the Responsible Director and shall escalate all material incidents, issues, risks, suspicious transactions and any other matters deemed relevant by the MLRO.
10. The Responsible Director shall be responsible for the appointment and termination of the AMLCO. The Responsible Director shall undertake a performance evaluation of AMLCO annually.

Annex II

Customer Acceptance Policy (CAP)

1. Purpose

The purpose of this Policy is to provide guidance and clarity on customer acceptance policy of the company and to ensure compliance with all applicable legal and regulatory requirements and framework.

2. Customer Acceptance Principles

The evaluation of a customer's risk is fundamental to the Company's effort to prevent and suppress money laundering, terrorist financing and other illegal activities.

The company reserves its right to deny the establishment of any business relationship with a person (physical and/or legal) assessed to fall within the groups of not accepted customers described below or indeed if for any reason the company is uncomfortable with the establishment of a business relationship.

The BPS Customer Acceptance Policy (CAP) is designed to ensure that the company adequately assesses prospective and existing customers from an AML/CTF perspective in order to ensure that it establishes and maintains relationships with customers with no ML/TF relationships or transactions. In parallel, the CAP covers areas outside the Company's risk appetite, where a business relationship cannot be accepted.

BPS transact only with customers meeting minimum risk assessment criteria and without significant failure as per their AML policy and manual.

3. List of conditions under which a business relationship with an existing customer must be terminated

BPS may terminate Business relationship with an existing customer if the following conditions apply:

a) If during the review of the review/customer update process, the customer fails or refuses to provide vital information requested by the company.
b) If a court order by the local authorities (or external/Lithuania) has been issued against a customer, resulting in an unacceptably increased ML/TF risk associated with the customer.
c) If the customer's activities change, and the new activities fall within the Company's non-accepted types of business or customers.
d) If a customer was convicted for any serious predicate offence.
e) If a customer has attempted to deceive the company.

f) If a customer becomes a subject to specific sanctions (i.e. EU, UN, OFAC, local lists), including close family members, close associates and related entities (irrespective of the percentage of ownership, either direct or indirect, held by the entities subject to sanctions).

g) If so requested by PAYRNET or supervisory authorities.

4. Customers (natural or legal entities) NOT Acceptable for BPS

The below list is not an exhaustive list of not Accepted customer types and might change from time to time.

a) Carries out illegal activities (such as human trafficking, drug dealing, child pornography, pedophilia, fraud or illegal arms dealing etc.).
b) Is convicted for a crime included in the predicate offences covered under the relevant law in each jurisdiction.
c) Fails to provide adequate identification and information or to disclose its financial operations.
d) Is a shell company, a shell bank or a bank which deals with shell banks or shell companies.
e) Is a terrorist or deals with terrorist activities (such as financing terrorist activities etc.).
f) Request to have accounts in the name of anonymous or fictitious persons.
g) Is from a political regime not recognized by the United Nations.
h) Is subject to specific sanctions (i.e. EU, UN, OFAC, local lists), including close family members, close associates and related entities (irrespective of the percentage of ownership, either direct or indirect, held by the entities subject to sanctions).
i) Is acting on behalf of or dealing/trading with any sanctioned persons or is involved in any sanctioned activity.
j) Is an individual customer whose country of residence is outside the EU (in the future).
k) Is a Politically Exposed Person (PEP), for whom the source of wealth cannot be determined or the reasoning of establishing a business relationship with us is not clear.
l) Is a customer who engages in the following business which are considered as prohibited:
    - Unregulated financial services (where likening required);
    - Pyramid of Ponzi scheme or multi-level marketing programs;
    - Hawala;
    - Un-licensed FX broker;
    - Binary options;
    - Debt restructuring, credit repair, debt settlement, providing credit, debt collections (unless received a written pre-approval from Company's Management Board);
    - Gambling [1];
    - Get rich quick scheme [2];
    - Activities aimed at circumventing security controls (software, hardware)
    - Unregulated pharmaceuticals / food supplements (e.g. "nutraceuticals") [3];
    - Piracy or illegal streaming;
    - Counterfeit goods and violation of intellectual property, items that violates someone's privacy;
    - Arms / dual use goods / human organs;
    - Unlicensed charities;
    - Shell companies;

- Companies formed of Bearer Shares;
- Remittance funds in cash; cash and check handling: check cashing, deposit talking, cash transfer;
- Offshore bank transactions / shell banks [4];
- Adult services connected to human trafficking; intermediation of prostitution; production, visual broadcasting of pornography or striptease clubs (the approach does not include literature, toys, DVD's, educational or scientific material or dating sites);
- Fourth party payment and multi-layered MSB arrangements;
- Transactions for goods subject to export prohibition/restrictions;'
- Transactions with living animals (exceptions possible like for payments for horse riding, or dog classes);
- Political / religious organizations engages in hate speech [5];
- Sanctioned entities;
- Un-licensed Crypto-asset activities [6].

Where:

[1] Gambling and any similar activity with an entry fee and/or monetary prize, including, but not limited to casino games, sports betting, horse or greyhound racing, fantasy sports, lottery tickets, other ventures that facilitate gambling.

[2] Short term investment for very high return.

[3] Drugs, narcotics, steroids, other products with danger to health. Homemade alcoholic beverages, cigarettes and tobacco.

[4] Offshore refers to the EU commissions tax evasion blacklist and grey list https://ec/europa.eu/taxation_customs/tax-common-eu-list_en. Any exceptions need to be approved by the MLRO

[5] Selling, hosting, distributing, producing or promoting offensive materials, including materials that incites racial discrimination based on gender, race, religion, national origin, physical ability, sexual orientation, age.

[6] No digital ledger / trading, only payment gateway (for Bitcoin, Bitcoin Cash, Ethereum, tether, Litecoin and Ripple).

5. Examples of directly High-Risk customers (natural or legal persons)

Although, the categorization of a customer as high risk is based on the overall score assigned from all the factors that are being taken into consideration some customers are being directly flagged as high-risk customers.

The following classifications of customers which are directly designated as high-risk customers and subject to EDD measures during the onboarding process as well as ongoing monitoring:

- Politically Exposed Persons
- "Customer Accounts" in the name of third persons
- Complex structured companies
- Correspondent/respondent relationships with banks not regulated in the EEA (currently not applicable)

Annex III (UAB "PAYRNET" Guidance to Customers)

KYB/C - UAB "PAYRNET" guidance to customers

Below is a list of requirements for UAB "PAYRNET". UAB "PAYRNET" is aware that businesses vary in size, nature and technical capability. Therefore, it's key to note that the below are **guidelines** for conducting KYB/C. Firms should follow a risk-based approach and base their KYB/C on regulatory requirements and adapt their methods based on findings measured in their Business Wide Risk Assessment (BWRA).

Firms are welcome to deviate from these guidelines so long as this is measured appropriately. PAYRNET, where deviation occurs, will want to verify the change by analysing the BWRA points to gain assurance that the KYB/C procedures mitigate and prevent risk, aswell as establish data for use of appropriate monitoring.

Where firms are unsure on how they conduct a BWRA they should seek external help. KYB/C must be tailored as appropriate to prevent key financial crime risks. Relevant information and checks should be added where necessary. Further information can be foundin Lithuanian Law on the Prevention of Money Laundering and Terrorist Financing.

Remember: KYB/C is a fundamental AML control and must be constructed to prevent financial crime (e.g. identifying key risk indicators), and to collect information to support monitoring. Information on the customer must be collected and validated. This information isneeded to not only identify and verify the customer but assess the level of risk posed. Therefore, it is important to assess what information gives enough indication of the customers expected behaviors.

In summary, for both KYB and C, you must:

- Identify the customer – collect information to know exactly who is responsible for the account (where non-face to face onboarding is used, this increases risks of impersonation or money mules). The identity of someone is commonly considered unique where you gain name, date of birth and address. E.g. There may be two John Smiths born on the same day but two John Smiths born on the same day with different addresses makes them both unique. For corporate customers it's key to ensure that you identify the unique business and relevant information to show it has been incorporated legally. Its key is also to understand the nature of business to ensure that monitoring around the customer is adequate.
- Verify the identity – based on the above, you should verify as much as necessary which eliminates risk. For non-face to face identification of customer or customer's

representative use 3rd party IT tools with live photo/video verification service option. The minimum standard would be name, address and date of birth, commonly through ID Document and proof of address from two separate sources. One should be with name/address, the other with name/date of birth. Deviation from this is possible however the verification method should be as reliable as the common standard. Deviation is usually done where the above isn't possible (e.g. where a person doesn't physically have a proof of address). For corporates you should verify the business information (e.g. its on companies house).

- Assess the risk – once you have collected all information and verified whatever is relevant to eliminate risks you need to give a risk score and this should direct howoften, and how strictly, you monitor them. This should include considerations of:
    - The geographic region/jurisdiction the customer resides in (does this have high rates of specific financial crime exposure?)
    - The product - can the product used be the customer be exposed to specific things?
    - The deliver channel - how does the way you are delivering the product increase risk?
    - The customer - does the customer themselves pose any direct risks?
    - The transactions - if the customer wants to do specific transactions to certain countries or just in general, are there specific risks associated with them?

  Using the above you should measure your risk based on a weighted score. This is for you to define based on your product offering.

PAYRNET recommendations

Below is a good KYB/C approach. It may not apply to you in areas so please assess each step. If you are saying I don't want to do that step ask yourself why not? If you still think it doesn't apply you have to be able to explain why and show you have measured this risk. When you measure the risk have you used a reliable and explainable methodology? KYB/C must protect you from financial crime so if you are considering a challenge to one of the below ensure that you know that it’s irrelevant and why.

Business:

- Information/Documentation required:
    - Official (government issued) or notarised Certificate of Incorporation and Memorandum/Articles of Association; or Pull an electronic version of the above containing the following information: Business name, Legal form, Registered address, Actual (or trading) address, Registration number (also called Legal code register number), registration date, nature of business (this can be gathered from the customer directly).
    - Official (government issued) or notarised document of share ownership shows the ultimate shareholders (e.g. share allotment, share certificate issued by the government business registry etc.) including any appointed director of the company; or Pull an electronic version from a reliable source, which pulls the information from the different companies house used on a periodic basis (monthly), including the following information: most up to

date ownership (showing the relevant ownership percentage, this depending on the risk level per end user) and list of directors. If ownership or list of directors is not verified through the above methods, a notarised document by external independent (not part of the company) registered lawyers or accountants must be provided.

    - Source of funds and wealth (audited financial statements, bank account statements, dividends, other proof).

Please note that, Shareholders of 25% or greater control over the end user are classed as UBO s (except for high risk end users, where 10% will need to be checked)

- Directors:
    - In date government Photo ID document or driver's license issued in an EEA member state.
    - If citizenship of the individual is not within the ID document provided, this information needs to be given for each individual.

- UBOs/Shareholders:
    - In date government Photo ID document or driver's license issued in an EEA member state.
    - If citizenship of the individual is not within the ID document provided, this information needs to be given for each individual.
    - Proof of address, this can be a utility bill, personal bank statement, or any equivalent document issued by central or local government authority, department or agency; This must be obtained, unless the address can be verified electronically (2+2 check).
- 3rd Party Checks:
    - Business - Screen the company against PEP, sanctions and Adverse Media.
    - Directors - Verify the ID provided by each director and their identity by using a live photo/video transmission verification service.
    - Directors - Screen the individual against PEP, Sanctions and Adverse Media.
    - Intermediaries in Ownership Structure - Screen the company against PEP, sanctions and Adverse Media
    - UBOs - Verify the ID provided by each UBO.
    - UBOs - Address verification (2+2).
    - UBOs - Screen the individual against PEP, sanctions and Adverse Media.

Individuals:

- Information/Documentation required:

    - In date government Photo ID document or driver's license issued in an EEA member state.

    - If citizenship of the individual is not within the ID document provided, this information needs to be given for each individual.
    - Proof of address, this can be a utility bill, personal bank statement, or any equivalent document issued by central or local government authority, department or agency; This must be obtained, unless the address can be verified electronically (2+2 check).
    - Identification documents and identity needs to be verified via live photo/video transmission service.
- 3rd Party Checks:
    - Individual - Verify the ID provided and their identity by using a live photo/video transmission verification service.
    - Individual - Address verification (2+2).
    - Individual - Screen the individual against PEP, sanctions and Adverse Media.

ANNEX IV - HIGH RISK AND PROHIBITED COUNTRIES LIST

Sanction country	Country code	Prohibited country	Country code	High risk + EDD	Country code	High risk	Country code
Afghanistan	AF	Belarus	BY	Nigeria	NG	Algeria	DZ
Crimea	N/A	Central African Rep	CF	Puerto Rico	PR	Angola	AO
Cuba	Cu	Congo, the Democratic Republic	CD	Saudi Arabia	SA	Antigua and Barbuda	AG
Iran, Islamic Republic of	IR	Eritrea	ER	Sri Lanka	LK	Armenia	Am
North Korea	KP	Ethiopia	ET	Tunisia	TN	Azerbaijan	AZ
Syria	SY	Republic of Guinea	GN			Belize	BZ
Venezuela	VE	Iraq	IQ			Benin	BJ
		Lebanon	LB			Bolivia	BO
		Liberia	LR			Bosnia-Herzegovina	BA
		Libya	LY			Brazil	BR
		Mali	ML			British Virgin Islands	VG
		Myanmar	MM			Burundi	BI
		Pakistan	PK			Cape Verde	CV
		Russian Federation	RU			China	CV
		Somalia	SO			Colombia	CO
		South Sudan	SS			Comoros	KM
		Sudan	SD			Curacao	CW
		Ukraine	UA			Dominica	DM
		Yemen	YE			Dominican Republic	DO
		Zimbabwe	ZW			Ecuador	EC
		Bahamas	BS			Egypt	EG
		Botswana	BW			El Salvador	SV
		Ghana	GH			Gaza Strip	PS
		Panama	PA			Guatemala	GT
		Barbados	BB			Guinea Bissau	GW
		Cambodia	KH			Haiti	HT
		Iceland	IS			Honduras	HN
		Jamaica	JM			India	IN
		Mongolia	MN			Kazakhstan	KZ

		Nicaragua	NI			Kenya	KE
		Uganda	UG			Kosovo	XK
		Albania	AL			Kyrgyzstan	KG
		Mauritius	MU			Lao People's Democratic Republic	LA
		Guam	GU			Mexico	MX
		American Samoa	AS			Moldova	MD
		Samoa	WS			Montenegro	ME
		Trinidad & Tobago	TT			Morocco	MA
		United States Virgin Islands	VI			Mozambique	MZ
		Cayman Islands	KY			Paraguay	PY
		Palau	PW			Philippines	PH
		Vanuatu	VU			Serbia	RS
		Seychelles	SC			Sierra Leone	SL
		Fiji	FJ			St Kitts & Nevis	KN
		Oman	OM			St Lucia	LC
						St Maarten	SX
						St Vincent & Gren	VC
						Tajikistan	TJ
						Tanzania	TZ
						Thailand	TH
						Turkey	TR
						Turkmenistan	TM
						Uzbekistan	UZ
						Vietnam	VN
						West Bank (Palestinian Territory)	PS
						Western Sahara	EH

Risk level	Trading address	Registration address	Residency Address	Owner / Director residency	Send / Receive Money	EDD on All Payments
High + EDD	Yes	Yes	Yes	Yes	Yes	Yes
Prohibited	No	No	No	Yes	No	No
Sanctioned	No	No	No	No	No	No

ANNEX V – ACCEPTABLE EVIDENCE OF SOURCES OF WEALTH AND FUNDS

Type of funds	Details required	Documentary Evidence required (original or fully certified copy)
1. Income-savings from salary (basic and/or bonus)- if self-employed or company share owner refer to 4 below	All of the following: Salary per annum Employer's name Address of business Nature of business	One of the following: Payslip (or bonus payment) from the last three months Letter from employer confirming salary on letter-headed paper Bank statement showing clearly showing receipt of most recent regular salary payments from named employer
2. Sale of investment / liquidation of investment portfolio	All of the following: Description of shares / units / deposits Name of seller How long held Sale amount Date funds received	One of the following: Investment / savings certificates, contract notes, or surrender statements Bank statements clearly showing receipt of funds and investment company name Signed letter detailing funds from a regulated accountant on letter–headed paper
3. Sale of Property	All of the following: Sold property address Date of Sale Total sale amount	One of the following: Letter form a licenced solicitor or regulated accountant stating property address, date of sale, proceeds received, and name of purchaser Copy of Sale contract
4. Company Sale	All of the following: Name and mature of the company Date of Sale Total sale amount Customer's share	Letter detailing company sale signed by a licensed solicitor or regulated accountant on letter headed paper Copy of contract of sale, plus bank statement showing proceeds, copies of media coverage (if applicable) supporting evidence
5. Inheritance	All of the following: Name of deceased Date of death Relationship to customer Date received Total amount Solicitors details	One of the following: Grant of probate (with a copy of the will) which must include the value of estate Copy of will Letter from lawyer or trustee

6. Divorce settlement	All of the following: Date and total amount received Name of divorced partner	One of the following: Copy of the court order Letter detailing divorce settlement signed by a licensed solicitor on letter headed paper
7. Company profits	All of the following: Name and address of the company Nature of company Amount of annual profit	One of the following: Copy of the latest audited company accounts Confirmation of the nature of business activity and turnover detailed in a letter from a regulated accountant
8. Retirement income	All of the following: Retirement date Details of previous occupation/profession Name and address of the employer Details of pension income source	One of the following: Pension statement Letter from an regulated accountant Bank statement showing receipt of latest pension income and name of provider Savings account statement
9. Fixed Deposits/Savings	All of the following: Name and institution where savings account is held Date the account was established Details of how the savings were acquired	All of the following: Savings statement Evidence of account start (letter from the account provider) Additional evidential information can be requested in relation to the origin of the savings held
10. Dividend payments	All of the following: Date of receipt of dividend Total amount received Name of company paying dividend Length of time the shares have been held in the company	One of the following: Dividend contract note Bank statement clearly showing receipt of funds and name of company paying dividend If dividend is payable from the customer's own company, one of the following Letter detailing dividend details signed by a regulated accountant on letter headed paper Set of company accounts showing the dividend details
11. Gift	All of the following:	Letter from donor confirming details of gift If PEP Documented evidence of donor's source of wealth as laid out in this table

	Details of date and amount of gift Details of person making gift – ID and occupation details for PEP/Sanctions screening Reason for gift and the nature of the relationship to the individual making the gift	
12. Loan	All of the following: Name of loan provider Date and amount of loan	One of the following: Copy of the Loan Agreement and details of any security Copy of loan statements
13. Lottery/Gambling Win	All of the following: Name of source Details of Windfall	One of the following: Evidence from the lottery company Cheque Winnings' receipt
14. Compensation Payout	Details of events leading to claim	One of the following: Letter/court order from compensating body Solicitor's letter
15. Life Insurance/general insurance payout	All of the following: Amount Received Policy Provider Policy Number/reference Date of payout	One of the following: Payout statement Letter from insurance provider confirming payout

ANNEX NO 6 – FORMS OF LOGS

FORM OF LOG
OF SUSPICIOUS OPERATIONS OR TRANSACTIONS AND REPORTS SUBMITTED TO PAYRNET

No.	Date of entry	Customer						Representative of the customer (if any)			Data about monetary operation or transaction			Criteria due to which monetary operation or transaction is considered as suspicious	Beneficial owner			Receiver of funds					Date when Report was submitted to PAYRNET
		Natural person			Legal entity													Natural person		Legal entity			
		Name, surname	Citizenship	Personal code (for foreigner – date of birth)	Name, legal form	Registered Office address	Legal code (if any)	Name, surname	Citizenship	Personal code (for foreigner – date of birth)	Date of the Monetary Operation or transaction	Description of the Property related to the Monetary Operation or transaction	Value of the Property*		Name, surname	Citizenship	Personal code (for foreigner – date of birth)	Name, surname	Date of birth	Name, legal form	Registered Office address	Legal code (if any)	

Amount of funds, currency in which the monetary operation or transaction is performed, market value of the property.

FORM OF LOG
OF SUSPICIOUS OPERATIONS OR TRANSACTIONS AND REPORTS SUBMITTED TO PAYRNET

No.	Date of entry	Customer						Representative of the customer (if any)			Data about monetary operation or transaction			Criteria due to which monetary operation or transaction is considered as suspicious	Beneficial Owner			Receiver of funds					Date when Report was submitted to PAYRNET
		Natural person			Legal entity													Natural person		Legal entity			
		Name, surname	Citizenship	Personal code (for foreigner – date of birth)	Name, legal form	Registered Office address	Legal code (if any)	Name, surname	Citizenship	Personal code (for foreigner – date of birth)	Date of the Monetary Operation or transaction	Description of the Property related to the Monetary Operation or transaction	Value of the Property*		Name, surname	Citizenship	Personal code (for foreigner – date of birth)	Name, surname	Date of birth	Name, legal form	Registered Office address	Legal code (if any)	

Amount of funds, currency in which the monetary operation or transaction is performed, market value of the property.

FORM OF LOG
ABOUT CLIENTS WITH WHOM BUSINESS RELATIONSHIP WERE TERMINATED DUE TO ML / TF RELATED CIRCUMSTANCES

No.	Date of entry	Customer						Representative of the customer (if any)			Beneficial owner			Motives due to which Business relationships were terminated under Article 18 of Lithuanian AML Law or based on other ML / TF related circumstances
		Natural person			Legal entity									
		Name, surname	Citizenship	Personal code (for foreigner – date of birth)	Name, legal form	Registered Office address	Legal code (if any)	Name, surname	Citizenship	Personal code (for foreigner – date of birth)	Name, surname	Citizenship	Personal code (for foreigner – date of birth)	