



AML POLICY

CONTENT:

- I. Purpose – BPS CYP LTD as distributor of PAYRNET
 - II. AML/CTF Procedures and controls
 - a. What is Money Laundering?
 - b. What is Terrorism?
 - c. Obligations
 - III. Risk appetite statement
 - IV. Risk based approach
 - a. Business Wide Risk Assessment
 - b. Customer risk assessment
 - V. PEPS
 - VI. KYC/B minimum requirements during the onboarding process (CDD)
 - VII. Enhanced Due Diligence (EDD)
 - VIII. Suspicious Activity Report (SAR)
 - IX. Record Keeping
 - X. International sanctions
- Annexes

Cyprus Office:

20 CHARALAMBOU MOUSKOU STREET, ABC BUSINESS CENTRE, 5TH FLOOR OFFICE 506,

PAPHOS, 8010, CYPRUS

Company Registration Number: HE 300214



1. PURPOSE – BPS CYP LTD AS DISTRIBUTOR OF PAYRNET

Blueberry Payment Solutions (BPS CYP LTD) is committed to the highest standards of anti-money laundering (“**AML**”) and counter-terrorism financing (“**CTF**”) compliance (collectively “**AML**”).

BPS CYP LIMITED (“BPS”) is registered in Cyprus as a Limited Company, with Registration Number HE300214 and operating as an appointed distributor of UAB “PAYRNET” (further – **PAYRNET**), which is incorporated in Lithuania and authorized as an Electronic Money Institution in Lithuania. To this extent, BPS must also follow and apply certain Lithuanian and Cypriot legal requirements, including those deriving from Lithuanian and Cypriot 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.

2. AML/CTF PROCEDURES AND CONTROLS

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

Cyprus Office:

20 CHARALAMBOU MOUSKOU STREET, ABC BUSINESS CENTRE, 5TH FLOOR OFFICE 506,

PAPHOS, 8010, CYPRUS

Company Registration Number: HE 300214

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, tax evasion, etc.

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 is 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.



WHAT IS TERRORIST FINANCING?

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 help 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 account holder'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 account holder business or type.

OBLIGATIONS

Cyprus Office:

20 CHARALAMBOU MOUSKOU STREET, ABC BUSINESS CENTRE, 5TH FLOOR OFFICE 506,

PAPHOS, 8010, CYPRUS

Company Registration Number: HE 300214



The issuer of the Blueberry 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 the related payment services.

Blueberry Payment Solutions (BPS CY LTD) acts as program manager for the 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.

It is BPS's responsibility and obligation to ensure that, where applicable, local-host state AML/CFT laws are applied when providing services in a jurisdiction other than Cyprus under the distributor's status. BPS, as previously mentioned must comply with the Cypriot and Lithuanian National AML Law which are in line with the requirements of the Directive (EU) 2015/849 of the European Parliament and the updated Directive (EU) 2018/843. Additional Lithuania-specific requirements that may be imposed by PAYRNET must be also followed.

Cyprus Office:

20 CHARALAMBOU MOUSKOU STREET, ABC BUSINESS CENTRE, 5TH FLOOR OFFICE 506,

PAPHOS, 8010, CYPRUS

Company Registration Number: HE 300214



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's AML/CFT requirements have been met.

BPS, acting as a distributor of PAYRNET, is required to apply AML requirements 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

Management and communication of information in connection with implementation of AML/CTF requirements.

3. 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:

Cyprus Office:

20 CHARALAMBOU MOUSKOU STREET, ABC BUSINESS CENTRE, 5TH FLOOR OFFICE 506,

PAPHOS, 8010, CYPRUS

Company Registration Number: HE 300214



- 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 with regulators;
- 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 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 I**).

4. KYC/B MINIMUM REQUIREMENTS DURING THE ONBOARDING PROCESS

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. Additionally, BPS should collect the information necessary to understand the purpose and intended nature of the customer's relationship with the company.

NECESSARY INFORMATION

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

Cyprus Office:

20 CHARALAMBOU MOUSKOU STREET, ABC BUSINESS CENTRE, 5TH FLOOR OFFICE 506,

PAPHOS, 8010, CYPRUS

Company Registration Number: HE 300214



- 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;
- 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 to 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, Residence Permit (if applicable).



* Proof of address refers to any of the following: Utility bill, local authority tax bill or a bank statement (not online bank) or any other document same with the aforesaid

The above information and documents are to be received during remote identification – through photo/selfie (not cropped) or real-time video transmission.

LEGAL PERSONS

Representative of the legal person must go through the same process as natural person, i.e. information (i.e. ID document) to be received during remote identification – through photo/selfie (not cropped) or real-time video transmission.

In addition, in the 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, contact numbers, 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.



5. RECORD KEEPING

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

The time limits for record keeping may be additionally extended for no longer than two years upon a reasoned instruction of a competent authority	
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)	8 years as of the day of the end of the Business relationship with the customer
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

6. 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@blueberrycard.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 the 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 the 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 A 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 becomes 0 (zero) Euro 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 the above paragraphs immediately thereafter.

Cyprus Office:

20 CHARALAMBOU MOUSKOU STREET, ABC BUSINESS CENTRE, 5TH FLOOR OFFICE 506,

PAPHOS, 8010, CYPRUS

Company Registration Number: HE 300214

ANNEX I – CUSTOMER ACCEPTANCE POLICY (CAP)

1. PURPOSE

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

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 the 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:

If during the review of the review/customer update process, the customer fails or refuses to provide vital information requested by the company.

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.

If the customers activities change, and the new activities fall within the Company's non-accepted types of businesses or customers.

If a customer was convicted for any serious predicate offense.

If a customer has attempted to deceive the company.

If a customer becomes 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).

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.
- Carries out illegal activities (such as human trafficking, drug dealing, child pornography, pedophilia, fraud, or illegal arms dealing etc.).
- Is convicted for a crime included in the predicate offenses covered under the relevant law in each jurisdiction.
- Fails to provide adequate identification and information or to disclose its financial operations.
- Is a shell company, a shell bank, or a bank that deals with shell banks or shell companies.
- Is a terrorist or deals with terrorist activities (such as financing terrorist activities etc.).
- Request to have anonymous accounts or in the name of fictitious persons.
- Is from a political regime not recognized by the United Nations.
- 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).
- Is acting on behalf of or dealing/trading with any sanctioned persons or is involved in any sanctioned activity.
- Is an individual customer whose country of residence is outside the EU/EEA.
- 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.
- 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);
- Activities aimed at circumventing security controls (software, hardware)
- Unregulated pharmaceuticals / food supplements (e.g. "nutraceuticals") [1];
- 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 [2];
- 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 [3];
- Sanctioned entities;
- Un-licensed Crypto-asset activities [4].

Where:

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

[2] 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

[3] 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.

Cyprus Office:

20 CHARALAMBOU MOUSKOU STREET, ABC BUSINESS CENTRE, 5TH FLOOR OFFICE 506,

PAPHOS, 8010, CYPRUS

Company Registration Number: HE 300214



[4] 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 (currently not applicable)
- Complex structured companies
- Correspondent/respondent relationships with banks not regulated in the EEA(currently not applicable)