Client Due Diligence and Platform-Partner Due Diligence Policy

Online Payment Platform Ltd.

Summary

The Client Due Diligence (CDD) and Platform Partner Due Diligence (PPDD) Policy of Online Payment Platform (OPP) defines the Policy for the onboarding and acceptance of Clients and Platform-Partners and the monitoring of the future relationship within the context of AML compliance.

Version: 6.0

Versioning

Version	Date	Changes	Owner
1.0	2019-01	A comprehensive review of CDD policy on PSD2	
1.1	2019-02	Domestic PEP adjustment and governance approval	
1.2	2019-03	Textual adjustments	
1.3	2019-10	Adding crypto and crowdfunding platform policy	
1.4	2020-10	Update the legal name and translate it into English	
1.5	2021-02	The closing policy and geographical scope added, updated identification of UBOs	
1.6	2021-06	Geographical scope modified Added roles and responsibilities	
2.0	2022-03	General update / periodic review	
3.0	2022-11	CDD/PPDD Policy and procedure separated, and a new structure for the OPP Group	CRO
4.0	31 May 2023	Update to make UK specific	CRO
5.0	2023-09	Update in prep for FCA application resubmission	CCO
6.0	29 May 2025	Annual review	CRO

Contents

1. Introduction

Online Payment Platform focuses on facilitating payment services on platforms and marketplaces. Platforms (including trading platforms and marketplaces) are the new form of e-commerce and the sharing economy. They add value by connecting supply and demand. OPP agrees with these platforms to integrate OPPs software solutions, including payment services. These partners are called Platform-partners.

Users on platforms can be individuals and legal entities, depending on the platform's proposition. These platforms are generally and preferably involved in the entire process of matching supply and demand, including the financial transaction, without being part of the agreement between the buyer and seller themselves. These parties are called Clients.

For these platforms, OPP integrates payment and e-money services and a selection of additional (payment and e-money related) services, such as (multi) split payments, escrow, and fraud detection. OPP directly offers these regulated services to the merchants and buyers (clients) of the platforms. By providing our service directly to the users, the platforms are shielded from providing payment services themselves, and we also ensure that these platforms process less personal data.

For UK clients OPP can also offer e-wallets on the

platforms. This policy only covers the activities of OPP UK

Ltd.

There is a wider OPP Group of companies and for context this consists of OPP Netherlands too - a Dutch registered Payment Initiation company that provides payment facilitation services to European customers across multiple EU countries. They have previously provided their services to UK Platforms and Merchants under the Temporary Permissions Regime ("TPR"). This UK activity ceased upon OPP UK Ltd being registered and Authorised by the FCA.

In order for OPP to operate within its risk appetite OPP must have a good understanding of its Clients so that a reasonable opinion can be formed whether or not they are involved in any fraudulent or illegal activities (fraud, money laundering, terrorist financing etc.). To achieve that, each Client is subject to a Client Due Diligence process that meets our risk based approach and regulatory/legal requirements and aligns with the Client's complexity and inherent risks of OPP's products and services. The Client risk is systematically reviewed through periodic and event-driven Client reviews. The requirements for the CDD process are presented below.

CDD must be fully completed, the Client must be identified and verified, and the Client's risk level must be defined before providing payment services.

There are various types of users (clients) on the Platforms to which this CDD Policy applies

- **legal entities** acting as merchants by offering their services on the platform;
- **individuals acting** as merchants by offering their services on the platform;
- **legal entities** acting as buyers on the platforms opening an e-wallet (UK only), and
- **individuals** acting as buyers on the platforms opening an e-wallet (UK only).

A user can have both roles of merchant and buyer on a platform. As implemented per platform, the due diligence process can have an integrated approach where the due diligence requirements will cover both roles. However, this is decided per platform.

1.1 Purpose

OPP is serious on its reputation and wishes to drive a viable, sustainable and legal business. Therefore, the company is firmly committed to preventing the use of its products and services for

money laundering or facilitating other criminal or terrorist financing activities. OPP identifies, manages, and mitigates financial and economic crime-related risks, such as money laundering and terrorist financing, through this policy.

This document outlines OPP's Client Due Diligence (CDD) and Platform Partner Due Diligence (PPDD) Policy. This Policy applies to all clients entering a business relationship. For OPP Ltd, this CDD/PPDD Policy, therefore also applies to the buyers where e-money services are provided.

The Policy ensures that OPP has an effective framework to identify risks of financial and economic crimes concerning OPP's Clients through appropriate due diligence. Appropriate due diligence means proportionate and considering both the nature and the scope of the activities undertaken by OPP.

Platform partners are essential for the product proposition of OPP, and they can materially determine the Client's risk profile. Therefore, these partners must undergo a Platform Partner Due Diligence (PPDD) process too. This process is described in the Platform Partner Due Diligence Procedure.

1.2 Approvals

This Policy, and any revision thereof, is subject to approval by the management board of OPP. Any amendments in the future must also be approved by the Board. The owner of this Policy is the CRO, and it is this role that will provide annual and periodic review of this policy together with recommended amendments to the policy over time.

1.3 Scope

This CDD/PPDD Policy application is mandatory for all employees and the OPP management boards. The Policy applies to all existing and new Clients and Platforms. A revision of this policy can lead to a review of all clients. The CDD/PPDD Policy will also apply to any future outsourced service providers for CDD-related processes to the extent relevant.

1.4 Regulatory framework

The CDD/PPDD Policy reflects the relevant requirements and recommendations relating to the prevention of financial and economic crime, i.e. money laundering, terrorist financing and sanctions adopted by the authorities of the United Kingdom, the European Union (EU)and the further worldwide community where relevant.

The following overview summarises the laws, regulations, and guidelines OPP has considered while drafting this policy.

1. Payment Services Regulations 2017;
2. The Money Laundering, Terrorist Financing and Transfer of Funds Regulations 2017, amended by The Money Laundering, Terrorist Financing (Amendment) Regulations 2019;
3. The Terrorism Act 2000;
4. The Anti-terrorism, Crime and Security Act 2001;
5. The Wire Transfer Regulation;
6. The European Banking Authority (EBA) revised ML/TF Risk Factors Guidelines of 1 March 2021;
7. The Counter-terrorism Act 2008;
8. The Proceeds of Crime Act 2002;
9. Bribery Act 2010;
10. JMLSG Guidelines;
11. FCA Financial Crime – a Guide for Firms; and
12. System and Control (SYSC) Rules of the FCA Handbook.

OPP UK Ltd will also implement relevant guidance by the Financial Action Task Force (FATF) in its policies and operational procedures.

1.5 OPP risk appetite ML/TF

The CDD/PPDD Policy must adequately manage relevant risks that the Client or Platform-Partner may entail. The risks that may influence the relationship with a Client or Platform-Partner include: integrity risk, derived integrity risk, fraud risk and the risks of (unintended) involvement in money laundering and terrorist financing.

OPP's risk appetite for Money Laundering and Terrorist Financing has been established in the Risk Management Framework - we have zero appetite or tolerance. In the Systematic Risk Assessment (SRA), the risks of money laundering and terrorist financing (ML/TF) in relation to OPP's business activities have been analysed. These two documents are the frameworks on which this CDD/PPDD Policy was built. It lays the foundation for the CDD and PPDD process as explained in this Policy and the related procedures.

Exceptions

Client or Partner relationships or transactions that would otherwise breach this CDD/PPDD Policy – but are not in violation of applicable laws – may be permitted in specific circumstances. In those cases, one-off exceptions may be given by the Board of OPP UK Ltd in conjunction with advice from the Head of Compliance.

Breach of Client Due Diligence Policy

Failure to comply with this CDD/PPDD Policy and associated policies and procedures will result in disciplinary actions. In determining the level of disciplinary action, the offence's seriousness and frequency will be considered by the Board of OPP UK Ltd.

Implementation

This CDD/PPDD Policy has been translated into controls, operational procedures and work instructions. All processes, procedures, and work instructions are subject to a regular review to ensure they reflect the necessary controls to manage the risks determined in the SRA adequately.

Training and Awareness

Training is an ongoing process incorporating developments and changes to applicable regulations and country requirements. The training also covers changes to internal policies, procedures, processes, and monitoring systems. Training reinforces the importance that OPP management attaches to compliance and will ensure that all employees understand their role in maintaining an effective CDD and PPDD process.

OPP will provide the necessary training, procedures, and material to make employees aware of their obligations and enable them to comply with this Policy and legal/regulatory obligations. In addition, all employees have a personal responsibility to ensure that they know this Policy and the accompanying procedures and comply with the requirements.

This Policy will be circulated periodically to the relevant personnel who make use of this policy and subsequent processes to ensure they are up to date with its contents and any changes/amendments that are made. This policy will be reviewed annually at a minimum and when any amendments have been made sooner.

2. Definitions

Account	In cases where the OPP's payment services user has access to an online environment where transactions, user data and settings are displayed.
Alert	An Alert will be generated in case of deviation from the expected transaction or client data.
Business relationship	A relationship between OPP and its Platform partners and Merchants.
Buyer not paying with e-money	A natural or legal person with whom OPP has no business relationship.
Buyer paying with e-money	A natural or legal person with whom OPP enters a business relationship for the provision of an e-wallet.
CDD risks	- Reputation risk; the risk that may arise due to adverse publicity. - Operational risk; the risk of damage resulting from non-compliance with the procedures drawn up by OPP. - Legal risk: litigation, criminal prosecution, damages and other sanctions threatening the continuity. - Concentration risk: the risk of (unconsciously) doing too much business with persons or companies that ultimately belong to the same conglomerate.
Client	A natural or legal person with whom a business relationship as a Merchant or Buyer is entered into for the provision of payment or e-money services.
client acceptance policy	Adequate control measures should reduce CDD risks to a manageable level. OPP must make choices about CDD based on carefully conducted risk analyses.
client research	This research aims to understand the nature and background of a relationship, as far as is reasonably possible, to determine whether there are any risk-increasing circumstances. Different circumstances and factors will be taken into account for each relationship. Based on the information collected, it will be assessed whether OPP wishes to do business with the relevant relationship.
Compliance level	Different levels of client research in OPP's systems.
Head of Compliance	The Compliance Officer is responsible for ensuring we are compliant with UK regulations as stipulated by the FCA.
Consumer account	Account intended for individuals not acting on behalf of a company.
Crowdfunding	A method of financing that makes use of multiple public funders. Used for multiple reasons including good causes.
Cryptocurrency	Virtual currency enables payments between users to be made without the involvement of a central authority or financial institution.
Client Due Diligence (CDD)	Gaining sufficient insight into the nature and activities of OPP's clients. OPP performs this CDD on a risk-based approach per specific legislation and regulations. The CDD policy must adequately manage the relevant risks associated with client services. The client acceptance process consists of the following components: identification, verification, acceptance, monitoring, and review.
e-money	Electronic money represents a monetary value that is stored electronically or magnetically for future use.
FATF	The Financial Action Task Force (FATF). It is an intergovernmental body aiming to achieve cooperation and coordination at the international level to prevent and combat money laundering and terrorist financing.
Terrorist financing	The intentional acquisition or possession of objects of financial value to commit a crime; the provision of financial support and the intentional raising of money for the benefit of an organisation to commit a crime.
High-risk country	A country identified as having insufficiently established a system to prevent money laundering and terrorist financing. OPP uses the FATF's, European Commission's and the UK's current lists to identify high-risk countries.
Merchant	A natural or legal person offering goods or services on the platform of a Partner
Partner risk analysis	The findings concerning the relationship with the Partner. Based on this analysis, the risk category for the users registered on the platform is determined based on the

	characteristics of the relationship, the products and services, the expected transaction characteristics, and the type of users.
Platform	Online e-commerce or sub-economy environment where supply and demand are brought together. This can involve both private and business parties.
Platform-partner	The Partner enters a partnership with OPP and integrates OPP's services onto its platform.
Politically Exposed Person (PEP)	A PEP is a natural person who holds or has held the next prominent public office less than a year ago: (a) Heads of State or Government, Ministers and Secretaries of State; (b) Members of Parliament; (c) members of supreme courts, constitutional courts and other high courts delivering judgements against which no further appeal is possible, except in exceptional circumstances; (d) members of courts of auditors or central bank boards of directors; (e) ambassadors, chargé d'affaires and senior army officers; (f) members of the administrative, management or supervisory bodies of public undertakings. g) the immediate family members (parents, spouse, registered Partner, children and their spouses or partners) and persons known to be close associates of the person mentioned above shall be considered to be Political Prominent Persons.
Review	The data and risk category of the existing Client is checked for accuracy and timeliness based on the (possibly changed) information about the Client available at that time.
Risk classification	Dividing clients into different risk categories.
Risk categories	Based on the Client's characteristics, the services and products offered by the Client and the initial risk category identified during the Partner risk analysis, the Client is assigned to one of the three risk categories identified by OPP: low, standard, or high.
Risk-based client research	Adjusting the depth and regularity of client research based on the relevant Risk category.
Sanction list	Warning lists identifying persons, entities or countries with deficiencies in their anti-money laundering and counter-terrorist financing systems or based on political decisions to put pressure. OPP uses the sanction lists of the following organisations: - National terrorism sanction lists (NL, UK) - European Commission (EU Freeze list) - United Nations - OFAC The sanction lists are updated at least monthly by OPP.
Transaction limits	Representation of the Client's expected transaction volumes.
Transaction monitoring	Monitoring is the continuous monitoring of the Client and the transactions carried out during the business relationship. In this case, it means checking whether any signals make a review or notification of an unusual transaction necessary.
Ultimate Beneficial Owner (UBO)	A natural person who holds an interest of 25% or more of the capital interest or 25% or more of the voting rights of the shareholders' meeting or who is otherwise able to exercise 25% or more effective control in the legal entity.
Verification	Establish that the identity given corresponds to the true identity.
Business account	Account intended for clients representing a legal entity.
Business relationship	Business, professional, or commercial relationship between OPP and a natural or legal person related to OPP's payment service activities.

3. Roles and responsibilities

3.1 Three lines model – an integrated approach

OPP is organised in line with the three lines of defence model. The three lines of defence model ensures a broad integral approach with cooperation between the different departments.

1st line: Management, Business and (KYC)
Support 2nd line: Compliance team
3rd line: Internal Audit

3.2 First line functions – Management Board

The management board is responsible for the following:

- Defining the AML governance and risk management framework,
- The overall implementation and effective operation of the AML framework,
- Implementing and executing this CDD/PPDD Policy, including the implementation, execution and testing of procedures related to the CDD/PPDD Policy requirements,
- Setting and propagating the appropriate tone at the top,
- Fostering an open environment for employees to discuss potential violations of this CDD/PPDD Policy,
- Ensuring that training is developed and delivered to the relevant employees for this CDD/PPDD Policy and the broader FEC framework, and
- Ensuring record retention requirements are met.

Management board approval is required for the following:

- Amending this CDD/PPDD Policy,
- Accepting all Partners and all new clients that are assessed as high risk, or continuing the relationship with partners and clients that have been re-evaluated as high risk, and
- Approving exceptions to this CDD/PPDD policy.

3.3 First line functions – Business and Support

The first-line employees of the business and support teams (and the management board) are responsible for the following:

- Complying with this CDD/PPDD Policy,
- Understanding how this CDD/PPDD Policy relates to their function and responsibilities,
- Knowing how to react when they become aware of behaviours that potentially breach this CDD/PPDD Policy, and
- Seeking advice from the compliance function or their manager(s) in case of questions about this CDD/PPDD Policy or when procedures require their advice or approval.

The business and support team conducts Client surveys and reviews of (i) Platform-partners, (ii) merchants (both individuals and legal entities), and (iii) buyers who wish to open an e-money account. They are responsible for the CDD process and making a proper risk assessment. Current measures and any additional mitigating measures are assessed.

Clients can be accepted directly by the first line, in line with this CDD/PPDD policy and related procedures (Risk Appetite for Platform Partners doc). If the client due diligence reveals that a client is a high risk due to specific indicators, advice should be sought from the second line, with the decision of whether to approve from an onboarding perspective being taken by the Board.

A high-risk client can be accepted (only by the Board) based on positive advice from the second line. If the advice is negative or is assessed as a potentially unacceptable risk, the decision is made by senior management only.

Currently, the management board must always approve new Platform-partners regardless of risk profile. this will be kept under review and lower risk Platform Partner approvals may be delegated in the future.

It is ensured that the first line receives sufficient information to carry out their tasks and responsibilities regarding Client or Platform-partner research and onboarding. This is done through the training given internally by the compliance teams and management, courses from various recognised training bodies, work descriptions and appropriate authorities in the system and external CBT by our external suppliers.

It is important that the first line have:

- Access to the (personal) data of the merchant for CDD purposes;
- Information that enables us to makes the decision of acceptance of Clients (merchants and the UK buyers in case of e-money);
- Contact with Clients if additional questions result from the CDD;
- The information available to them for the business to Prepare a risk assessment of a client;
- the ability to request internal advice and report findings if there is an increased risk.

3.4 Second line – compliance team

The second line Compliance team is responsible for the following:

- Ensuring implementation and, after that, monitoring the effectiveness and execution of this CDD/PPDD Policy and related procedures,
- Providing advice to the first line on the implementation and execution of this CDD/PPDD Policy,
- Reporting on the effectiveness of the CDD governance and risk management framework to the management board, and
- Ensuring that effective operational risk management processes are in place.

The Compliance team's advice is required for the following:

- The acceptance or review of Platform-partners and clients that are assessed as high risk,
- The acceptance or review of Platform-partners or clients that may involved in sanctions or who are active in high-risk countries and/or may be classified as a PEP;
- Platform-partner or Client exit decisions;
- Answering requests for information from regulators or other authorities, and
- Escalating to the Board exceptions to this CDD/PPDD Policy.

The compliance team works with the first line and supports it with advice, as described in the first line.
The compliance team is responsible for periodically monitoring the execution and control of the CDD/PPDD process by the first-line employees. The compliance officer's monitoring program specifies what is monitored and with what frequency. The client files are randomly assessed for the completeness of the client due diligence. Signals of possible shortcomings and the results thereof are reported to the management as these reviews take place.

The compliance team also drafts and seeks Board approval for any adjustments to the CDD/PPDD Policy. The Policy is assessed annually and occasionally revised, for instance, in the event of changes in the legislation and regulations. In the event of changes, the compliance officer shall advise the Management Board through a revised version of the Policy, after which the Management Board, as the party with final responsibility, shall assess it. The compliance officer

communicates any changes that impact the frontline staff's work to the wider team and confirms to Management that this has been completed.

Second line responsibilities:

- Access the (personal) data of the merchant for CDD or Platform-partner for PPDD to assist with advice and guidance or review;
- Preparing internal work descriptions and procedures relating to this policy;
- Drafting for board approval and adjusting after board approval the CDD/PPDD framework;
- Providing training to all relevant employees;
- Checking the control of the client research and giving advice when requested by first line;
- Access to Ruler concerning risk management;
- Transaction Monitoring oversight and challenge (via Sentinels tool);
- Reporting unusual transactions to the National Crime Agency (NCA);
- Passing on advice and findings to the first line (and management where necessary/appropriate) when there is an increased risk.

A detailed explanation of the interpretation and control of the compliance function is laid down in the compliance charter.

3.5 Third line - audit

Third Line reviews the implementation and application of this Policy and that the second line has performed their Compliance Monitoring Plan reviews and action to ascertain that it is sound, effective, and applied across the business. The audit review process is outlined in agreed-upon procedures and the audit planning.

Due to the size and complexity of OPP UK Ltd we have not yet appointed an Internal Audit function within the business. The Board will keep this under regular review and appoint a Third Line of Defence Audit function when it is appropriate to do so - this will be lead by the Firms CRO.

4. Due Diligence framework

4.1 Introduction Due Diligence

There are two elements of DD that OPP performs - that is PPDD and CDD. These are the applicable requirements when onboarding Clients or Platform-partners and have been outlined in this section.

Every Platform-partner or Client is subject to PPDD or CDD based on requirements that may differ depending on OPP risk indicators and services provided to the Client or Platform-partner.

The PPDD and CDD will identify financial, propositional and economic risks to determine whether the Client or Platform-partner can be accepted in line with OPP's risk appetite as described in the Firm's Risk management Framework.

4.2 For which relationships must PPDD or CDD be performed?

Platform-partners

Platform-partner onboarding forms the basis of the related merchant onboarding. A merchant is always associated with a specific Platform-partner. If a merchant also uses another Platform that OPP works with they will have to go through a CDD process each time. For each Platform-partner, we perform a specific risk assessment. We assess activities on the platform, such as products traded, type of merchants (legal entity vs. individuals), merchant characteristics, preferred payment methods and associated risks, expected transaction size, number of transactions per merchant and total trading amount per merchant. Based on this analysis, we capture merchant-specific risk levels that will be applied for the merchants' verification and transaction monitoring of this Platform-partner.

In addition to the above analysis, we identify UBOs and verify legal representatives, company registration with Companies House, bank account ownership and VAT registration.

We also require Platform-partners to state and substantiate whether they have policies for anti-bribery/anti-corruption, fraud prevention, anti-money laundering, compliance with accounting and tax laws, economic sanctions, sustainability and diversity. We also ask them to confirm how they manage these topics and that they have appropriate measures, policies and procedures to manage and monitor the above concerned risks. If they do not have such policies we wish to understand why not and what they will be doing to have them in place prior to going live with OPP.

Furthermore we continually review our Platform Partners to ensure we continue to be satisfied that the business model they have and operate remains within the risk appetite of OPP. We also ensure that the individuals and nature of the corporate entity that owns and manages the Platform are also within the risk appetite of OPP - please see below for more information on ongoing reviews of Platform partners.

Please refer to the Platform Partner Onboarding Application form for further detailed questions of what we require for Platform partner onboarding.

Clients – Merchants and Buyers

OPP has identified the following clients it will enter a business relationship:

- Merchants receiving payments from the buyers – legal entities (companies) and individuals (consumers);
- Buyers (consumers) who wish to open an e-wallet account.

An important part of our activities is the onboarding of merchants. Merchants who wish to offer products on a platform and receive payments for delivered goods or services need to be identified and verified before a transaction can be settled or their e-wallet can be used. We identify and verify merchants, which can be individuals or legal entities, as part of our client acceptance process. Depending on the risk assessment of the Platform-partner and the merchant's risk profile, the identity is verified through bank verification, ID verification or an extended verification (for legal entities) - see below for further information.

5. Client risk rating

5.1 Introduction

The Client risk rating is determined by combining the outcomes of the risk assessment of four risk categories, namely:

1. Client risk;
2. Country risk;
3. Product and services risk; and
4. Delivery channel risk.

The risk categories are subdivided into risk factors per risk category. Those risk factors must be considered when establishing the risk assessment per risk category.

5.2 Client risk

Client risk is primarily driven by client types and characteristics associated with:

- the Client's legal form;
- the Client's ownership and control structure;
- the Client's economic ownership, voting rights or other forms of control (UBO);
- results from the adverse media checks;
- PEP involvement;
- sanctions targets;
- the Client's sector; and
- the Client's previous behaviour (registration on the Internal Signal List).

These factors combined will result in the Client risk rating, which can be low, standard, high or unacceptable.

Ownership and control structure

A client's ownership and control structure may be qualified as complex if:

- the structure involves offshore jurisdictions (e.g. tax heavens);
- the ownership structure includes an unusual amount of ownership layers;
- the ownership structure includes offshore trusts; or
- the Client has a complex share/shareholder structure.

If a Client's ownership structure qualifies as complex OPP will take additional measures to ensure that it has adequately established and verified the ownership (UBO) and control structure. OPP will also establish the Client's rationale for using such complex structures and understand them before making a decision to onboarding them.

Risk factors

The table below displays which risk indicators should be considered when assessing the Client risk.

Client risk assessment				
Risk factor	**Low risk**	**Standard risk**	**High risk**	**Unacceptable risk**
Legal form	Natural persons	Legal entities (e.g. LTD's, LLPs, PLCs)	Trusts, foundations	No insight into trustees or beneficiaries
Ownership and control structure	N/a	The Client does not have a complex ownership structure	The Client has a complex ownership structure and has a valid reason for such a structure	The Client has a complex ownership structure and has no valid reason for such a structure
Client economic ownership, voting rights or other forms of control (UBO)	N/a	The UBO is clear and acceptable	The UBO is unclear, or the UBO is linked to adverse media (EDD must be applied)	The UBO is unclear, or the UBO is regarded as not acceptable by Executive Board decision
Adverse Media	No Adverse media detected	No Adverse media detected	True hit on Adverse media relating to the Client or Associated Parties (EDD must be applied)	The board decides if the hit on adverse media is considered unacceptable
PEP	No PEP identified	No PEP identified	True hit on PEP relating to the Client, or Associated Parties (EDD must be applied)	The board decides if they want to provide services to the PEP or if the PEP is considered unacceptable
Sanctions	No Sanctions identified	No Sanctions identified	True hit on sanctions but not relating to services provided by OPP - move to decline	True hit on sanctions relating to the Client or associated parties for the services provided by OPP - this will result in a declined application
Client sector	Not mentioned in Annex IV	Not mentioned in Annex IV	See Annex IV; high-risk sectors	See Annex IV; prohibited sectors
Internal signal list	Not on the internal signal list	Not on the internal signal list	True hit on the signal list, but board decides that the services can be provided	True hit on the signal list and relation determined unacceptable

A true hit on Sanctions is an unacceptable risk, and further reference should be made to the Sanctions Screening Policy, where we will decline this application. In case of a true hit on a PEP or adverse media, Enhanced CDD must be applied, and the Client risk rating must be 'high' or unacceptable and only Board approval is ankle to be provided for these cases to progress with their application.

5.3 Country risk

Country risk can be described as the risks associated with the Client's residence or statutory seat or where the Client has business activities or the beneficiary's country.

The country risk can be considered low if a client is established (or has business activities) in the EEA or UK.

If a client is established (or has business activities) in or has citizenship in a high-risk country (see annex II), the country risk and the Client risk rating must be considered 'high', and Enhanced CDD must be performed.

OPP maintains a list of countries it considers high-risk due to the higher risk of criminal activities, such as money laundering or terrorist financing or the lack of AML/CTF standards (please refer to Annex II). OPP also maintains a list of countries it considers an unacceptable risk (please refer to Annex III).

Country risk assessment				
Risk factor	**Low risk**	**Standard risk**	**High risk**	**Unacceptable risk**
Country of residence or statutory seat and (if applicable) place(s) of business activities	The Client is situated in the EEA or UK	The Client is not situated in a high-risk country	The Client is situated in a high-risk country, as stated in OPP high-risk country list	The Client is situated in an unacceptable risk country, as stated in OPP unacceptable risk country list

In the case of a client from a high-risk country, the Client's source of funds or wealth must be identified and verified.

Settlement of the client money is only settled on UK bank accounts.

5.4 Product and services risk

OPP provides financial services to the Merchants of the Platforms and e-money wallets to buyers in the UK.

Essentially there are two elements of pay-out risk that we consider at OPP; Low and Standard and the differentiator of the two are the size and frequency of payments. For any payment that is below £250 or a cumulative £2,000 in any 12 months we apply our Low Risk measures; whereby we only confirm the ownership of the Bank Account when paying out monies - preferable using our AIS capability with the Platform Partner.

For all payments over £250/£2,000 cumulative we perform KYC, Bank Account ownership and activity validation checks whereby we will check the Consumer activity on the Platform to ensure they are not operating a business using a consumer account - if we find such an activity we will work with the Platform to ensure that they restrict the users account and convert it to a Business accounts.

Below is a visual representation of the above levels of pay out risk we assess.

For Business Merchants we validate the Company and their bank accounts before paying out to them regardless of Risk factors - of course if there are high risk factors in place for the Merchant, like PEP, High Risk Country or Negative Media results then we will perform additional risk checks, similar to EDD checks.

Product/Services risk assessment				
Risk factor	**Low risk**	**Standard risk**	**High risk**	**Unacceptable risk**
Individual Merchant account	Up to 250 pound per payment or 2000 GBP lifetime payments	From 250 GBP per payment or 2000 GBP lifetime payments		
Business Merchant account	n/a			

Product/Services risk assessment				
Risk factor	**Low risk**	**Standard risk**	**High risk**	**Unacceptable risk**
E-wallets for UK buyers	Up to250 pound per payment or 2000 GBP lifetime payments	From 250 GBP per payment or 2000 GBP lifetime payments		
Platform-Partners	Government (related) platforms		X (Annex IV)	X (Annex IV)

5.5 Delivery channel risk

Delivery channel risk refers to how the Client obtains the products or services from OPP. In this regard, OPP offers its financial services on a non-face-to-face basis only. Therefore, OPP has taken additional measures to mitigate the higher risk of remote onboarding.

5.6 Client risk rating

The Client risk rating is determined by combining the risk assessment outcomes of the below three risk categories.

Client risk rating	
Client risk rating	**Outcome risk categories**
Low risk	The client is not a PEP or Sanctioned individual, and no other increased risk is identified
Standard risk	The Client is not a PEP, and a maximum of one increased risk is identified as per the above Risk Factors table
High risk	The Client is a PEP, or at least two other increased risks have been identified as per the above Risk Factors table

6. Required Client Due Diligence measures

The method of performing CDD and the applicable requirements differ between Clients based on their risk profile, the Platform-partner requirements and the platform risk from the PPDD. The PPDD risks are categorised as Simplified CDD, Standard CDD and Enhanced CDD. The CDD process is as follows:

1. OPP determines whether Simplified CDD, Standard CDD or Enhanced CDD applies, based on identified and estimated risks in relation to the Client and the categorisation requirements in this Policy;
2. OPP conducts appropriate CDD measures. If during the Standard CDD process additional risks are identified, then the process for Enhanced CDD must be applied as well; and
3. Following the initial CDD process and identifying the Client's risk rating, OPP will continue to monitor the Client's activities and perform periodical reviews.

We require an identification process for each separate Platform-partner. Hence, if a merchant is already registered for a specific platform, OPP will still perform the merchant onboarding process, as the risk profile of the Platform-partner and therefore the merchant can be different.

6.1 Simplified CDD

Simplified CDD on a can only be applied if the Client represents a low risk of money laundering or financing of terrorism.

Simplified CDD may not be conducted if:

1. adverse media has been found on the Client relating to money laundering, terrorist financing, fraud or other financial or economic crimes,
2. the Client, its ultimate beneficial owners (UBOs), the legal representative, or other associated parties are politically exposed persons (PEPs),
3. the Client is situated or has business activities in a high-risk country, or
4. there is a positive hit during the sanctions screening on the Client, its UBOs, the legal representative or other associated parties - in the case of a positive Sanction result the case will be escalated to the Board with a recommendation that it is declined.

Simplified CDD is the first step in the due diligence process and this applies to merchants that sell goods for a maximum value of 250 GBP per transaction and 2,000 GBP in lifetime transactions.

6.2 Standard CDD

Standard CDD is considered the default CDD procedure for clients and must be applied unless Simplified CDD or Enhanced CDD can or must be applied.

Standard CDD is as follows:

- Proof of Identity is required - valid Passport or Driving License;
- Proof of Residential Address is required - Utility Bill dated within the last 3 months;
- Proof of ownership of their Bank Account.

6.3 Enhanced CDD

Enhanced CDD must be applied if OPP has established that the relationship with the Client presents a higher risk of money laundering or the financing of terrorism. Enhanced CDD must be conducted if one of the following criteria apply:

1. adverse media has been found on the Client relating to money laundering, terrorist financing, fraud or other financial or economic crimes;
2. the Client, its UBOs, the legal representative or other associated parties are PEPs;

3. the Client is situated or has business activities in a high-risk country;
4. there is a positive hit during the sanctions screening on the Client, its UBOs, the legal representative or other associated parties;
5. the Client is considered high risk in the Client risk rating; or
6. the Client is registered on the Internal Signal List

7. Required PPDD measures/approach

OPP performs a standard process for the onboarding of Platform-partners, including a risk assessment to define the risk profile of the Platform-partner and the services offered or traded on the platform.

The risk assessment form consists of gathering and assessing the following information:

- General Information Partner
- Ultimate beneficial ownership
- Services
- Financial information
- Compliance information
- Documents checklist
- Risk Assessment

Further details on the CDD process are defined in the PPDD Procedure.

8. Timing of the CDD

All Clients of OPP are subject to CDD before establishing the client relationship. In other words, an unknown client may not make use of OPP's financial services as CDD has not yet been performed. The first line may decide to deviate from the above rule that CDD is required before establishing the client relationship if it is essential for not disrupting the provision of OPP's financial services to the Client and when this does not entail a risk of money laundering or financing of terrorism. This option is only available after the first line has received positive written advice from the Board.

9. Record retention

All data that must be recorded by law or due to internal rules will be recorded in such a way that they are transparent and kept for each relationship, during the relationship and up to 7 years after the relationship has ended or the last transaction has been carried out. After this period, all data will be anonymised or deleted from OPP's database.

10. Periodic client Review

Platform-partners and Clients are subject to periodic CDD reviews. These CDD reviews are triggered through i) events or ii) the passing of time.

10.1 Periodic review due to trigger events

Certain events may unfold during the Platform-partner's or Client's business relationship, triggering an additional CDD/PPDD review. OPP should be aware of such trigger events and act accordingly. Therefore, a review must be conducted to determine if a Platform-partner or Client should have a different risk rating. Trigger events are:

1. Changes in the Company form or name, business address, legal representative, bank account, Platform-partner's or Client's name, UBO, board members or client/country/product risk(s) - API notifications received from Companies House
2. Adverse media has been identified on the Platform-partner, Client or Associated Parties,
3. Positive PEP or Sanctions screening hit on the Platform-partner, Client, or Associated Parties - at onboarding or during our daily uploads from Open Sanctions and it includes both PEP & Sanction screening.
4. The Platform-partner or Client is involved in an unusual transaction as defined in the transaction monitoring Policy and Procedure,
5. A substantiated complaint or notification is received via our support system or helpdesk.
6. Fraud alert from a bank / authority

10.2 Periodic review due to expiration of time

All Platform-partners and Clients are subject to periodic CDD/PPDD review after a certain period has expired since the previous CDD/PPDD assessment was conducted. The frequency of such periodical CDD reviews is based on the Client risk rating.

Periodic review		
Client risk rating	**Frequency review merchant**	**Frequency review Platform-partner**
Low risk	Event driven only	n/a
Standard risk	Every five years	Every year
High risk	Every year	Every 6 months

Review status

Upon expiry of the review term, the Client status is automatically set to review status in our OPP admin system. This means that no pay-outs will be made to the Client until a review has taken place and OPP are comfortable with the review.

The review process contains the same steps and elements as the regular Client research. During the review, an assessment will be made as to whether the Client is still in the correct risk category, whether the data still match, and whether adjustments are needed in the account. These findings will be recorded in the Client's file.

11. Client exit process

If OPP determines, after re-performing a client risk rating or during a periodic review, that continuing the relationship with a Platform-partner or Client bears an unacceptable risk for money laundering or terrorist financing, OPP may decide to end the business relationship. Any such outcome of a risk rating or periodic review will be communicated to the Compliance function for review. If the Compliance function determines an unacceptable risk, they will advise the Board to terminate the relationship with that Platform-partner or Client - the decision is with the Board to approve the termination recommendation.

The Platform-partner or Client exit process entails giving the Platform-partner or Client notice of termination according to the relevant clauses in the agreement following a decision by the Board. If the termination is due to Money Laundering or other Financial Crime reasons we will terminate the relationship with immediate effect. All terminations that have been provided with a notice period will be placed on a 100% supervision and review process whereby all transactions will be monitored until the relationship has been terminated.

12. Review

This CDD/PPDD Policy is reassessed, reviewed and adjusted (subject to Board approval) every year by the Policy owner - as defined on page 2. The results of the SRA will feed into the policy review process. If required by changes made to the SRA or an incident has occurred, this Policy may be amended directly outside of the regular review cycle - any and all amendments will only be approved by the Board.

OPP will regularly revise this CDD/PPDD Policy in the context of the recommendations made by the Financial Conduct Authority (FCA) and other regulatory / policy making bodies to maintain the integrity of the financial system, on Anti Money Laundering (AML) standards and on Combating Financing of Terrorism (CFT).

Annex I: Lower level and higher level risk indicators

The following is a non-exhaustive list of factors and types of evidence of potentially lower risk clients:

1) client risk factors:
   a) public companies listed on a stock exchange and subject to disclosure requirements (either by stock exchange rules or through law or enforceable means), which impose requirements to ensure adequate transparency of beneficial ownership;
   b) public administrations or enterprises;
   c) clients that are residents in geographical areas of lower risk as set out in point (3).

2) Product, service, transaction or delivery channel risk factors:
   a) financial products or services that provide appropriately defined and limited services to certain types of clients so as to increase access for financial inclusion purposes;
   b) products where the risks of money laundering and terrorist financing are managed by other factors such as purse limits or transparency of ownership (e.g. certain types of electronic money).
   c) Products and services provided with purchase limits (i.e. max 2000 GBP per transaction)

3) Geographical risk factors:
   a) EU Member States;
   b) UK;
   c) As defined in the UK - Countries having effective AML/CFT systems;
   d) As defined in the UK - Countries identified by credible sources as having a low level of corruption or other criminal activity;
   e) Countries, based on credible sources such as mutual evaluations, detailed assessment reports or published follow-up reports, that have sufficient requirements to combat money laundering and terrorist financing consistent with the revised FATF Recommendations and effectively implement those requirements.

The following is a non-exhaustive list of factors and types of evidence of potentially higher risk clients:

1) client risk factors:
   a) the business relationship is conducted in unusual circumstances;
   b) clients that are residents in geographical areas of higher risk as set out in point (3);
   c) legal persons or arrangements that are personal asset-holding vehicles;
   d) companies that have nominee shareholders or shares in bearer form;
   e) cash-intensive businesses;
   f) the ownership structure of the company appears unusual or excessively complex given the nature of the company's business.

2) Product, service, transaction or delivery channel risk factors:
   a) products or transactions that might favour anonymity;
   b) payment received from unknown or unassociated third parties;
   c) new products and new business practices, including new delivery mechanisms and the use of new or developing technologies for both new and pre-existing products.

3) Geographical risk factors:
   a) countries identified by credible sources, such as mutual evaluations, detailed assessment reports or published follow-up reports, as not having effective AML/CFT systems;
   b) countries identified by credible sources as having significant levels of corruption or other criminal activity;
   c) countries subject to sanctions, embargos or similar measures issued by, for example, the Union or the United Nations;
   d) countries providing funding or support for terrorist activities or that have designated terrorist organisations operating within their country.

Annex II: High-risk countries

- FATF High-risk and other monitored jurisdictions
- EU policy on high-risk third countries
- UK HM Treasury Advice; Schedule 3ZA of the MLRs (link)

Annex III: Unacceptable risk countries

- Cuba
- Iran
- Syria
- Belarus
- Democratic People's Republic of Korea (DPRK)
- Russian Federation
- The Crimean Peninsula including Sevastopol
- Donetsk People's Republic (Donetsk) and the Luhansk People's Republic (Luhansk) regions of Ukraine

Annex IV: High-risk and prohibited sectors

OPP uses SIC and SBI codes as unique identifiers to determine which industries it deems to be:

- prohibited, meaning OPP will not do business with clients engaged in those industries, or
- high risk, meaning OPP automatically applies Enhanced Due Diligence (EDD) to those clients - Board approval MUST be sought before conducting conversations with these Clients - please see Platform Partner Onboarding documentation for further information.

Where a client or counterparty, at onboarding or as part of Refresh, is identified as engaging in a high risk or prohibited industry, the client must be referred to the MLRO.

Prohibited Industries:		
SIC Number (5-digit SIC 2007)	**SBI Codes**	**SIC Name**
01150	Not specific	Growing of tobacco
01700	01.7	Hunting, trapping and related services
05101	08.99	Deep coal mines
05102	08.99	Open-cast coal working
12000	12	Manufacture of tobacco products
14200	14.2	Manufacture of articles of fur
24460	Not specific	Processing of nuclear fuel
25400	25.4	Manufacture of weapons and ammunition
26600	26.6	Manufacture of irradiation, electromedical and electrotherapeutic equipment
30400	30.4	Manufacture of military fighting vehicles
38120	38.12	Collection of hazardous waste
38220	38.22	Treatment and disposal of hazardous waste
46350	46.35 or 46.21.7	Wholesale of tobacco products
92000	92	Gambling and betting activities without a (local) licence
not specified	not specified	Trading of non domestic animals
01500		Farming
Not specified		Narcotics

High-Risk Industries		
SIC Number (5-digit SIC 2007)	**SBI Codes**	**SIC Name**
01280	01.28	Growing of spices; aromatic; drug, and pharmaceutical crops
02100	02.1	Silviculture and other forestry activities
02200	02.2	Logging
06100	06.1	Extraction of crude petroleum
06200	06.2	Extraction of natural gas
07100	not specified	Mining of iron ores

07210	not specified	Mining of uranium and thorium ores
07290	not specified	Mining of other non-ferrous metal ores
08110	08.1	Quarrying of ornamental and building stone; limestone; gypsum; chalk, and slate
08120	08.1	Operation of gravel and sand pits; mining of clays and kaolin
08910	08.99	Mining of chemical and fertiliser minerals
08920	08.92	Extraction and agglomeration of peat
09100	09.1	Support activities for petroleum and natural gas extraction
16100	16.10.1	Sawmilling and planing of wood
19100	19	Manufacture of coke oven products
19201	19.2	Other treatment of petroleum products
19209	19.2	Other treatment of petroleum products (excluding petrochemicals manufacture)
20150	20	Manufacture of fertilisers and nitrogen compounds
20200	20.2	Manufacture of pesticides and other agrochemical products
20590	20.5	Manufacture of other chemical products n.e.c.
21100	21	Manufacture of basic pharmaceutical products
21200	21	Manufacture of pharmaceutical preparations
24410	24.41	Precious metals production
24420	24.42	Aluminium production
24430	24.43	Lead; zinc, and tin production
24440	24.44	Copper production
24510	24.51	Casting of iron
24520	24.52	Casting of steel
24530	24.53	Casting of light metals
28110	28.11	Manufacture of engines and turbines; except aircraft; vehicle, and cycle engines
28210	28.21	Manufacture of ovens; furnaces, and furnace burners
28921	28.92	Manufacture of machinery for mining
28922	28.92	Manufacture of machinery for mining; quarrying, and construction
30110	30.1	Building of ships and floating structures
30120	30.1	Building of pleasure and sporting boats
30300	30.3	Manufacture of air and spacecraft and related machinery
32120	32.12	Manufacture of jewellery and related articles
33150	33.15	Repair and maintenance of ships and boats
33160	33.16	Repair and maintenance of aircraft and spacecraft
35220	35.20	Distribution of gaseous fuels through mains
35230	35.20	Trade of gas through mains
38110	38.11	Collection of non-hazardous waste
38310	38.31	Dismantling of wrecks
43130	43.13	Test drilling and boring
46120	46.12	Agents involved in the sale of fuels, ores, metals, and industrial chemicals
46140	46.14	Agents involved in the sale of machinery; industrial equipment; ships, and aircraft
46342	46.34	Wholesale of wine, beer, spirits, and other alcoholic beverages
46370	46.37	Wholesale of coffee, tea, cocoa, and spices
46390	46.39	Non-specialised wholesale of food, beverages, and tobacco
46460	46.46.1	Wholesale of pharmaceutical goods

46711	46.71.1	Wholesale of petroleum and petroleum products
46719	46.71.3	Wholesale of other fuels and related products
46720	46.72	Wholesale of metals and metal ores
46750	46.75	Wholesale of chemical products
46760	46.76	Wholesale of other intermediate products
46770	46.77	Wholesale of waste and scrap
49319	49.39.1	Other urban; suburban or metropolitan area passenger land transport (not incl underground, metro, and the like)
49320	49.32	Taxi operation
49500	49.5	Transport via pipeline
50100	50.1	Sea and coastal passenger water transport
50200	50.2	Sea and coastal freight water transport
50300	50.3	Inland passenger water transport
50400	50.4	Inland freight water transport
51102	not specified	Non-scheduled passenger air transport
51210	51.2	Freight air transport
51220	51.2	Space transport
52241	52.24.1	Cargo handling for water transport activities of division 50
56101	56	Licensed restaurants
56102	56	Unlicensed restaurants and cafes
56103	56	Take-away food shops and mobile food stands
56210	56.1	Event catering activities
56290	56.2	Other food services activities
56301	56.3	Licensed clubs
56302	56.3	Public houses and bars
63910	63.91	News agency activities
68201	68.20.1	Renting and operating of Housing Association real estate
68202	not specified	Letting and operating conference and exhibition centres
77110	77.11	Renting and leasing of cars and light motor vehicles
77120	77.12	Renting and leasing of trucks
80100	80.1	Private security activities
80200	80.2	Security systems service activities
80300	80.3	Investigation activities
84210	84.21	Foreign affairs
84220	84.22	Defence activities
91040	91.04	Botanical and zoological gardens and nature reserves activities
93191	93.19	Activities of racehorse owners
94200	94.2	Activities of trade unions
94910	94.91	Activities of religious organisations
94920	94.92	Activities of political organisations