PayU AML Policy

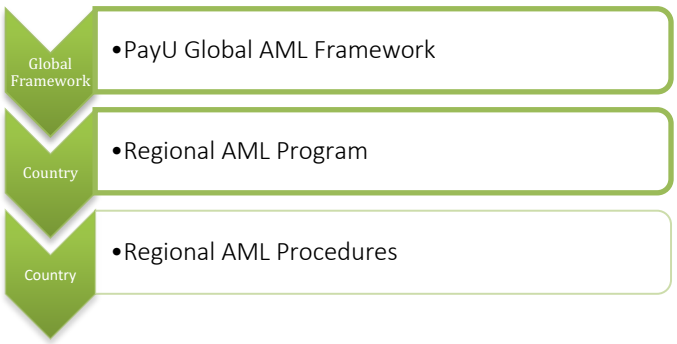
December 2019

As a payment service provider PayU Global B.V. and all of its subsidiaries (collectively referred to as *PayU*) operate in a highly regulated international environment. PayU is committed to conducting its business in accordance with applicable laws, rules, regulations, standards, codes and with proper regard for ethical business practices. In addition, it is PayU's policy to act in line with the standards and policies that are set by PayU's parent, Prosus N.V. (*Prosus*).

Introduction

PayU's AML program consists of the following two core pillars:

(i) PayU's Global AML Framework (this document);
(ii) Regional AML Program (appendixes);
(iii) Regional AML Procedures



When designing its AML framework, PayU has been cognisant of the importance of local compliance in the countries and markets it operates, and not just with a top down delegation of global policies that might not necessary address local country rules and regulations. PayU has therefore sought to balance its approach in the design and implementation of its AML framework.

A regional AML program will seek to identify any additional mandatory or different local obligations, map the laws and regulations that apply to the local business and the licence obligations imposed by its regulatory authority.

While PayU recognises the importance of a well-designed and complete AML framework, it is of paramount importance, that it is effectively implemented and percolated into the business at a local level. Details of how PayU goes about effectively implementing this in the country AML program are set out below.

International standards, laws and regulations require that PayU implements preventive measure to prevent money laundering, the collection of money or property for terrorist purposes or other criminal or fraudulent activities. PayU is fully committed to comply with the standards on anti-money laundering (hereinafter "AML") and counter-terrorist financing (hereinafter "CFT"). In addition, PayU is committed to review the PayU strategies and objectives on an ongoing basis in order to maintain an effective AML program. This policy sets on a high level the standards that PayU's management and employees must adhere to when establishing such rules and measures in accordance with a risk-based approach. The appendixes to this policy contain the more detailed regional AML programs and confirm the local standards of the regions that PayU is operating in.

Scope

The main purpose of the PayU AML program is to develop a minimum set of standards to prevent that the PayU setup will be used for money laundering (hereinafter "ML") or terrorism financing (hereinafter "TF") as it involves the handling of money. The PayU management team and all the PayU employees, contractors and subcontractors must adhere to the minimum standards that are laid down in the PayU AML program. In a jurisdiction where (local) laws or regulations set stricter rules than those set out in this policy, the stricter standards must be applied. If applicable laws are in conflict with this policy, the regional Legal and Compliance director must consult with the Global head of Compliance in order to resolve the conflict.
It is PayU's aim to review the PayU AML program on an on-going basis. The objective of this document is to provide information on how the PayU's AML program will assess, monitor, report and manage the ML and TF risks. The PayU

AML policy is intended to prevent that PayU and its employees are being misused for ML, TF or any other financial crime. Attached in the appendixes to the PayU AML program you will find the PayU regional AML programs. The scope of PayU's AML program is implemented in accordance with the following six elements:

1. Regulatory Framework
2. Risk Assessment
3. Merchant and beneficial owner identification, verification and risk profiling
4. Ongoing monitoring and record keeping
5. Reporting of suspicious transactions and asset freezing
6. Training

Regulatory framework

PayU operates in multiple countries and as such is licensed in some of these countries and supervised by the applicable regulatory body. The applicable regulatory framework for the PayU regions is found in the appendixes to this document. In addition to the applicable local laws and regulations PayU is committed to take the Financial Action Task Force ("FATF") recommendations into consideration by determining the PayU AML policy.

According to the definition of the FATF money laundering is defined as:

"The goal of a large number of criminal acts is to generate a profit for the individual or group that carries out the act. Money laundering is the processing of these criminal proceeds to disguise their illegal origin. This process is of critical importance, as it enables the criminal to enjoy these profits without jeopardising their source."

Money laundering consist of the following three stages:

- Placement: the physical disposal of cash or other assets derived from criminal activity.
- Layering: the separation of illicit proceeds from their source by layers of financial transactions intended to conceal the origin of the proceeds.
- Integration: 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.

These "stages" are not static and overlap broadly. Financial institutions may be misused at any point in the money laundering process.

Terrorist financing involves the solicitation, collection or provision of funds with the intention that these funds may be used to support terrorist acts or organizations. The funds may derive from both legal and illicit sources. According to the United Nations 1999 International Convention for the Suppression of the Financing of Terrorism, a person commits the crime of financing of terrorism "if that person by any means, directly or indirectly, unlawfully and wilfully, provides or collects funds with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out" an offense within the scope of the Convention.

Risk Assessment

Through the PayU Risk register PayU will identify, assess and understand the ML and TF risks. It is critical that the risk ratings accurately reflect the risks present and provide meaningful assessments that lead to practical steps to mitigate the risks. Based on the assessment PayU will apply a risk-based approach to ensure that the correct checks and controls are implemented to prevent or mitigate ML and TF risks. With the PayU Risk register PayU developed a thorough understanding of the ML and TF risks it faces when it comes to – but not limited to – PayU's merchants, products, services offered and the jurisdictions PayU and its merchants operate in. In addition to the Risk register PayU has implemented the PayU Compliance program that outlines the corporate governance structure of PayU and the three lines of defence approach. More information on the PayU Risk register, corporate governance and the three lines of defence can be found in the PayU Compliance program.

Merchant and beneficial owner identification, verification and risk profiling

PayU will - to the extent needed - perform the proper customer due diligence ("CDD") on the merchant, the person acting on behalf of the merchant and the beneficial owners of the merchant. The CDD is performed either before PayU enters into an agreement or before the first transaction is submitted to the PayU platform. PayU implemented a global CDD policy, depending on the merchants risk profile PayU will apply a risk-based approach and the performed due diligence will be simplified, standard or enhanced. The identification is done by - to the extent needed - obtaining the needed identification papers. Verifying the received information is done by using reliable, independent source documents, data or information. In addition to identifying and verifying the received information PayU will create an understanding on the nature of the merchants business, type of transactions and review the purpose of the relationship etc.

The minimum PayU CDD measures are in accordance with the FATF standards:

- Identifying the merchant and verifying the merchant's identity by using reliable, independent source documents, data or information.

- Identifying the beneficial owner, and taking reasonable measures to verify the identity of the beneficial owner. In addition understanding the ownership and control structure of the merchant.

- Understanding and, as appropriate, obtaining information on the purpose and intended nature of the business relationship between the merchant and PayU. Conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of the relationship to ensure that the transactions being conducted are consistent with PayU's knowledge of the merchant, their business and risk profile, including, where necessary, the source of funds.

Where any of the due diligence checks raise suspicion or reasonable grounds to suspect that the assets or funds may be the proceeds of offences related to ML or FT PayU will not approve the relationship and will file a suspicious transaction report with the relevant authorities.

PayU implemented a global Risk policy that reflects the PayU requirements to on-board new merchants. PayU identifies its risk appetite towards prohibited, low, medium and high-risk merchants and the acceptance of these merchants in the global Risk policy. PayU has a process in place to identify that where the risk for ML and FT is higher enhanced controls and checks are in place to mitigate and manage those risks. In addition to the PayU appetite with regard to accepting merchants there are situations whereby the chance for ML or FT is higher or lower considering the circumstances. In these situations enhanced or simplified CDD will be applicable.

On-going monitoring and record keeping

PayU has implemented among others the following monitoring procedures:

- The PayU risk register to effectively manage, monitor and mitigate any risks related to ML or FT. The PayU Risk department monitors the implementation of the correct controls to mitigate these risks.
- The bi-weekly/monthly PayU Compliance reporting to monitor compliance initiatives, regulatory changes, any known compliance deficiencies/issues, reported suspicious transactions and corrective action that has been taken through the bi-weekly PayU Compliance report. The PayU Global head of Compliance reports on these matters quarterly to the board of Prosus.

It is the aim of PayU to monitor its merchant to prevent ML and/or FT or any other criminal or fraudulent activities. A detailed monitoring overview for the PayU regions are found in the appendixes to this document.

PayU will ensure that all information and documentation that is requested to perform the CDD is correctly documented and stored. All information and documentation are to be kept in accordance with local regulatory requirements after the business relationship ended, or after the date of the occasional transaction. Upon appropriate request - determined by senior management - Payu will make the records available to the competent authorities.

Reporting of suspicious transactions and asset freezing

Proper CDD and monitoring may require PayU to gather further information regarding a merchant or a transaction before deeming it suspicious. The PayU employees are trained (see chapter 8) and policies are put in place in order to be able to monitor and review merchants and transaction in order to determine suspicious behaviour. PayU makes use of both internal and external tools to support it employees in detecting any suspicious behaviour. PayU implemented a risk-based approach based on - but not limited to - red flags to monitor and report suspicious activity.

Some of these red flags are:

- The information received from the merchant appears to be misleading, not complete or wrongly provided.
- The merchant's business profile does not match the transactions that are processed on behalf of the merchant.
- The merchant has an agent or financial advisor that acts on behalf of him without the proper documentation, such as a power of attorney.
- The merchant submits its CDD documentation showing an unclear ownership structure.
- The merchant submits unusual or suspicious identification documents or declines to provide the originals for verification or declines to provide certain documentation.
- The merchant is reluctant to reveal details about its business activities or to provide the financial statements.
- The merchant request the remittance to be transferred to an off shore bank account.
- Merchants that discuss record keeping or reporting requirements with the intention of avoiding them.

As PayU is a licensed institute in some of the countries it is operating in it is the obligation of PayU to report any suspicious transactions to the relevant authority. In the countries where PayU is not a licensed institute PayU will still monitor and if possible report any suspicious transactions. The details with regard to the reporting obligations of PayU can be found in the appendixes to this document.

PayU prohibits its employees to disclose the filling of a suspicious activity to the subject of the report or that a possible investigation is initiated.

Training

As PayU operates in a highly regulated + international environment and its focus is on the emerging markets the training and educating of all PayU's employees is a key impotent of the PayU's AML and Compliance policy. The PayU trainings and courses are tailored depending on the employee's role and region and will train and test employees and where needed third parties - among others - on relevant laws, regulations, PayU's policies and procedures and prohibited conduct. The PayU employees must pass a mandatory set of tailored courses at least once per year. The results of the mandatory courses are tracked and reported to middle management and to the PayU Global Management team. The training and online courses of PayU are updated regularly and the applicability of the training and online courses are reviewed by the relevant stakeholders at least ones per year. It is the aim of PayU to provide the employees where needed face-to-face training. The online trainings and courses are provided to the PayU employees through the PayU academy which is a web-based tool that makes it possible for all PayU employees to follow the online courses and trainings. Details with regard to which trainings and courses are incorporated can be found in the PayU Compliance policy.

Audit

The audit will be executed through the following three lines of defence approach, a more detailed description can be found in the PayU Compliance program:

- The first line of defence are the PayU employees
- The second line of defence are the PayU's Compliance departments and Risk departments.
- The third line of defence is the PayU internal audit department and the external auditor who report independently to the PayU Global Management team.