

Anti-Money Laundering Policy

Unicoin Limited, (Trading As) Wishu Anti Money Laundering and Counter Terrorist Financing Policy Statement

This policy sets out Wishu's commitment to understanding and minimising our risks in relation to money laundering and terrorist financing, so our services are not abused to legitimize the proceeds of crime. Our commitment to this strengthens our goals of achieving good ethical business and trading standards.

Our aim, by having robust policies and procedures and the creation of a compliance culture within the firm, is to prevent money laundering and terrorist financing.

In order to achieve this, we have undertaken the following:

1. Appointment of the nominated person/money laundering reporting office (MLRO)

The firm's MLRO is: James Johnson

Contact details

Internal mobile telephone extension: +447534788107

Email address: james@wishu.io

The MLRO is available to discuss any matters relating to the firm's policies and procedures relating to the Money Laundering Regulations and helping you understand your obligations. In the absence or sickness of the MLRO the following deputy/assistant MLRO has been appointed.

The firm's deputy/ assistant MLRO is: Hubertas Trinkunas

Internal mobile telephone extension: +447455901888

Email address: hubert@wishu.io

Introduction to the Policy

Wishu is required under the Money Laundering Regulations 2017 to put in place appropriate systems and controls to forestall money laundering and terrorist financing. This policy contains the procedures that we have developed in order to comply with these obligations.

The Money Laundering Regulations require that an organisation has a Nominated Officer to ensure that there is up-to-date knowledge of issues relating to Anti-Money Laundering and Counter-Terrorist Financing throughout the organisation, implement appropriate policies and procedures and receive reports of suspicious activity. The Nominated Officer (Money Laundering Reporting Officer) for *Wishu* is *James Johnson*.

Brief Definition

Use of the term “client” or “customer” refer to the users of the *Wishu* app.

“We”, “us” or “our” refer to *Wishu* and it’s staff members.

What is money laundering and terrorist financing?

Money laundering/ Terrorist Financing is the process by which criminals attempt to hide and disguise the true origin and ownership of the proceeds of their criminal activities (e.g. illegal drugs dealing, tax evasion etc.) thereby avoiding prosecution, conviction and confiscation of the criminal funds. The ultimate aim of this process is to convert such criminal proceeds into “clean” money. The risks to the financial sector primarily involve being used to facilitate this process, whether knowingly or unwittingly.

Key stages of money laundering

There are many ways of laundering money and these are deemed to be accomplished in three distinct stages:

Placement– this is the first stage in the money laundering operation and involves the physical disposal of the initial proceeds derived from illegal activity, e.g. placing cash in the conventional financial system

Layering– this second stage involves separating the illicit proceeds from their source by creating complex layers of financial transactions designed to disguise the audit trail and provide anonymity

Integration– the final stage involves providing an apparent legitimacy to the criminally derived wealth. If the layering process has succeeded, integration schemes place the laundered proceeds back into the economy in such a way that they re-enter the financial system appearing as normal business funds. The consumer credit sector can therefore act as a “safe haven” for criminal funds, allowing them to invest the proceeds of their criminal activities

These three steps may occur as separate and distinct phases and occur simultaneously or, more commonly, they may overlap.

Recognising and reporting suspicious transactions/activity

Individuals who handle, or are managerially responsible for handling, transactions which may involve money laundering must make a report promptly to the Money Laundering Reporting Officer (MLRO) with Wishu, if the individual knows or suspects or has reasonable grounds for knowing or suspecting that a customer is engaged in money laundering. Failure to follow the Policy may result in a personal criminal liability.

If the MLRO on review of the suspicion discovers that money laundering is taking place he will refer it to the National Crime Agency. A record of this will be kept.

Duty of staff in respect of money laundering Reporting of suspicious activity

If a member of staff comes across a transaction or an activity which is regarded as suspicious or unusual (or which could reasonably be regarded as such), then in the first instance, the Wishu Staff member should refer the transaction and/or activity in question without delay to the MLRO at Wishu.

The MLRO will consider the issue, together with any other relevant information available (including any information about the customer’s identity) and, if the suspicion is justified, make a report to the National Crime Agency

Any suspicion or knowledge of money laundering should immediately be reported to the MLRO

Client confidentiality

Once staff have made a report to the MLRO in accordance with staff legal responsibility, staff are protected under the law from being sued by the client for breach of confidentiality

- Please see Wishu's Privacy Policy for information relating to your data.

The 2007 Money Laundering Regulations ('the Regulations')

The Regulations require that the company establishes and maintains specific policies and procedures to guard against its business being used for the purposes of money laundering. They specify the range of procedures that the company should implement to fulfil this obligation.

Assistance

The combined effect of the UK statutes makes it an offence for any person to provide assistance to a money-launderer to obtain, conceal, retain or invest funds if he knows or suspects, or in the case of terrorist activities should have known or suspected, that those funds are the proceeds of an indictable offence.

Such assistance is punishable on conviction by a maximum of 14 years imprisonment or a fine, or both. It is a defence that the person concerned reported his knowledge or suspicion to the law enforcement agencies at the first available opportunity.

Tipping Off

It is also an offence for anyone to prejudice an investigation by informing the person who is the subject of a suspicion, or any third party, that a disclosure has been made, or that the police or customs authorities are carrying out or intending to carry out a money laundering investigation.

Making enquiries of a customer, to verify identity or to ascertain the source of funds for a particular transaction will not trigger a tipping off offence before a suspicious activity report has been submitted in respect of that customer. If a suspicious activity report has been made, great care should be taken to ensure the customer does not become aware of that fact.

The punishment on conviction for this 'tipping off' offence is a maximum of 5 years imprisonment or a fine, or both.

Failure to Report

In the case of drug trafficking or terrorist activity, it is an offence for a person who acquires knowledge or suspicion in the course of his trade, profession, business or employment not to report the knowledge or suspicion as soon as reasonably practical after the information came to his attention.

Failure to report in these circumstances is punishable on conviction by a maximum of 5 years imprisonment or a fine, or both.

The legislation protects those reporting suspicions of money laundering from claims in respect of any alleged breach of customer confidentiality.

Proceeds of Crime Act 2002

Part 7 of this Act consolidates existing UK Money Laundering Law. Significantly for the regulated sector there is now onus to report suspicions of money laundering where there are "reasonable grounds to suspect money laundering." This introduces an objective test on the regulated sector and reporting is not limited to circumstances where there is actual knowledge or suspicion of money laundering.

GUIDANCE AND COMMITMENT

The following points are our responsibilities under Money Laundering Supervision. These are how we will carry out checks on our business and customers, and what records we will keep to prevent money laundering.

Customer due diligence requirements

What is customer due diligence?

Customer due diligence means taking steps to identify our customers and checking they are who they say they are. In practice this means obtaining a customer's:

- Name
- Photograph on an official document which confirms their identity

- Residential address and date of birth
- Nationality
- Phone Number

Customers using our facilities will be required to use:

- A bank card with 3D secure authentication

3D security will be set at £0.01

In respect of moderated withdrawals, we will check information such as, name, KYC level, profile, history of deals, and transaction history (transfers, top ups and withdrawals).

The best way to do this is to ask for a government issued document like a passport, along with utility bills, bank statements and other official documents. Other sources of customer information include the electoral register and information held by credit reference agencies such as Experian and Equifax. Please be prepared to provide this if you are a customer.

If we have doubts about a customer's identity, we must stop dealing with them until we are sure.

When we need to apply customer due diligence measures

We must apply customer due diligence measures:

- When the user attempts to withdraw. In respect of refunds only, users of the Wishu app can only withdraw through transactions with another user. Previously topped up funds can only be refunded to cards used to initiate the topped up balance.
- when we establish a business relationship with a customer (or another party in a property sale)
- Customer Transactions worth less than €2,500 for cash-in and/or €1,000 for cash-out cumulated per legal year and per user (transfers are also counted in this equation)
- Transactions worth more than €2,500 for cash-in and/or €1,000 for cash-out cumulated per legal year and per user
- when we suspect money laundering or terrorist financing

- when we have doubts about a customer's identification information that we have obtained previously
- when it's necessary for existing customers - for example if circumstances change
- if we are not a high value dealer in a transaction, when we carry out an 'occasional transaction' worth €15,000 or more
- as a high value dealer, when we:
 - make a payment to a supplier worth €10,000 or more
 - carry out an 'occasional transaction' worth €10,000 or more

The changing circumstances of our customers

We need to keep up-to-date information on our customers so that we can:

- amend your risk assessment of a particular customer if their circumstances change
- carry out further due diligence measures if necessary

Changes of circumstance may include:

- a big change in the level or type of business activity
- a change in the ownership structure of a business

Internal controls and ongoing monitoring of your business

We will ensure that our business has adequate internal controls and monitoring systems. These will alert us and other relevant people in our business if criminals try to use our business for money laundering. Once we are aware of a potential threat, we will take steps to prevent it and report any suspicious activity.

Our controls include:

- Appointing a 'nominated officer' (headlining this document) and making sure that employees know to report any suspicious activity to them
- Appointing a compliance officer if your business is larger or more complex
- Identifying the responsibilities of senior managers and providing them with regular information on money laundering risks
- Training relevant employees on their anti-money laundering responsibilities
- Documenting and updating your anti-money laundering policies, controls and procedures
- Introducing measures to make sure that the risk of money laundering is taken into account in the day-to-day running of our business

Record keeping requirements

We need to keep a record of all customer due diligence measures that we carry out, including:

- customer identification documents
- risk assessments
- our policies, controls and procedures
- training records

By keeping comprehensive records we will be able to show that our business has complied with the Money Laundering Regulations. This is crucial to protect our business if there's an investigation into one of our customers.

The types of record we keep will include (if applicable):

- daily records of transactions
- receipts
- cheques
- paying-in books
- customer correspondence

The formats that we will keep our records in are:

- originals
- photocopies

- microfiche
- scanned
- computerised or electronic

You will keep our records for five years beginning from:

- the date a customer relationship ends
- the date a transaction is completed

Our Staff should and will not hesitate to report a suspicious activity to our MLRO - by failing to make a report staff are committing an offence. By not making a report, the firm and staff will not be able to take advantage of the protections afforded by the legislation.

Training

Who will receive training?

- All relevant staff will receive training.

What does the training involve?

- Training is provided through online courses.

It covers:

- The law relating to money laundering and terrorist financing
- Our policy and procedures
- Guidance on detecting money laundering and terrorist financing

Is completion of training compulsory?

- Completion of training is compulsory.

How often will training be provided?

- All new joiners will receive training as part of the induction process. Further training will be provided as required.

The Nominated Officer will continually monitor training needs but if you feel that you need further training on any aspect of the relevant law or our AML policy and procedures, please contact James Johnson.

MOVING FORWARD

We will review this policy at least annually as part of our overall risk management process.

We will also review this policy if:

- There are any major changes in the law or practice
- We identify or are alerted to a weakness in the policy
- There are changes in the nature of our business, our clients or other changes which impact on this policy

Where can I get further advice on AML/CTF matters?

You can get further advice and guidance from the Nominated Officer, James Johnson, or, in his absence the deputy, Hubertas Trinkunas.