ANTI-MONEY LAUNDERING ("AML"), COUNTER-TERRORIST FINANCING ("CTF") AND FINANCIAL CRIME POLICY

1. POLICY

1.1 Crixto Limited (the "Company") is exposed to the risk of criminals seeking to use the Company's business activities to launder money and commit other financial crimes. The Company and all its employees are subject to anti-money laundering and counter-terrorism finance laws, in particular the Proceeds of Crime Act 2002 ("POCA 2002") and the Terrorism Act 2000 ("TA 2000").

2. COMPLIANCE

2.1 All Company employees are expected to familiarise themselves with this policy and to comply with it.

2.2 Strict adherence to the provisions of this policy and other rules on anti-money laundering and counter-terrorist financing are a condition of employment by the Company. Any breach of this policy and such rules may result in disciplinary proceedings being taken against any relevant director or employee, and further may expose the individual concerned to the risk of criminal prosecution. In particular, failure to report knowledge or suspicions of money laundering to the Compliance Officer ("CO") when required is likely to be both a criminal offence, and to be regarded as gross misconduct which may result in immediate dismissal without payment. The board of directors, with the assistance of the CO, is responsible for initiating and supervising the investigation of all reports of breaches of this policy and other rules and ensuring that appropriate disciplinary action is taken when required.

3. WHAT IS MONEY LAUNDERING?

3.1 The Financial Action Task Force ("FATF") – an inter-governmental body of which the UK is a member, and which works to combat money laundering and terrorist financing - defines money laundering as follows:

3.2 "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…"

3.3 "When a criminal activity generates substantial profits, the individual or group involved must find a way to control the funds without attracting attention to the underlying activity or the persons involved. Criminals do this by disguising the sources, changing the form, or moving the funds to a place where they are less likely to attract attention.*"*

3.4 Typically, money laundering occurs in a number of stages.

3.4.1 First, in the initial - or placement - stage, the launderer introduces his illegal profits into the financial system. This might be done by breaking up large amounts of cash into less conspicuous smaller sums that are then deposited directly into a bank account, or by purchasing a series of monetary instruments (cheques, money orders, etc.) that are then collected and deposited into accounts at another location.

3.4.2 Secondly, after the funds have entered the financial system, a layering stage takes place. In this phase, the launderer engages in a series of conversions or movements of the funds to distance them from their source. The funds might be channelled through the purchase and sales of investment instruments, or the launderer might simply wire the funds

through a series of accounts at various banks across the globe. This use of widely scattered accounts for laundering is especially prevalent in those jurisdictions that do not co-operate in anti-money laundering investigations. In some instances, the launderer might disguise the transfers as payments for goods or services, thus giving them a legitimate appearance.

3.4.3 Thirdly, having successfully processed criminal profits through the first two phases, the launderer then moves them to the third stage – integration – in which the funds re-enter the legitimate economy. The launderer might choose to invest the funds into real estate, luxury assets, or business ventures.

3.5 The Company, through its acceptance of crypto-currencies in exchange for electronically stored balances of fiat currency which can be used for purchasing goods and services, is particular exposed to the second and third of money laundering.

4. RISK ASSESSMENT

4.1 In line with industry guidance, the Company understands that its anti-money laundering and financial crime measures should be risk proportionate, and designed to mitigate and manage the specific risks that are inherent in both its business and the particular transactions it is involved in. To this effect, the Company has carried out an AML and CTF risk assessment to identify risks to its businesses, and particular business activities that have higher risks.

4.2 This assessment is carried out on an ongoing basis and is updated as appropriate based upon changes to the business and its operations. A summary of the current risk assessments is as follows:

Overall risk assessment

4.3 Taking into account the FATF guidance, and other available information, the Company assesses the risk of its crypto-exchange and value transfer business being subject to money laundering or terrorist financing as moderate. The products which the Company offers are, by their nature, potentially attractive to money launderers (see further below), albeit at the lower end of the risk spectrum relevant to this industry.

4.4 The Company's activities which are exposed to the highest risk of financial crime are the primary activity of the business and carried out in a routine and high-volume basis. Whilst the Company does not receive in cash from customers, it does receive assets that may have been purchased using criminal property and then converts such assets into monetary value which can be exchanged for further assets. In these circumstances, the AML risk to the Company associated with these activities is materially the same as the AML risk associated with receiving cash directly from customers and transferring that cash on to third parties. The relative degree of anonymity involved in crypto-assets, as well as the fact that crypto-assets are not tied to specific jurisdictions and the non-face-to-face distribution channels used increases the risk factors for the Company.

Customer risk factors

4.5 The customers of the Company's services are mainly restricted in practice to individuals, but there are certain corporate clients. Customers can potentially be based in any location and are not restricted in their regulatory classification (i.e. the Company could deal with retail consumers carrying out one-off exchanges, as well as repeated professional crypto-asset users carrying out regular exchanges). As crypto-assets are not a common investment asset, and seeking to convert them into stores of fiat currency is not a typical service, it is unlikely that the Company's

customers can be seen as having a risk profile equivalent to other e-money and money remittance users

4.6 As identified in the Company's AML Risk Assessment, there is potentially a risk of Company entities coming into contact with "politically exposed persons" (as defined in the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 ("MLRs 2017")) during the course of its business, albeit this is relatively low.

4.7 A further potential risk is that the Company may not have ongoing relationships with customers, with some customers potentially engaging in one off transactions with the Company. This therefore limits the Company's opportunity to build up a range of data about the customer and their transactions to assist in identifying suspicious trends and the like. This is somewhat mitigated by the fact that exchanges will be directly connected to purchasing power as specific merchants, thereby giving a clear picture of who the value of the crypto-assets will ultimately be transferred to, albeit it does not completely mitigate the risk.

Countries and geographic risk factors

4.8 The Company's activities could have links to high risk jurisdictions. The Company itself carries out its activities in the UK, albeit customers and the transferred assets can originate from jurisdictions outside of the UK and EEA. The Company is therefore directly exposed to overseas jurisdictions (including non-FATF members).

4.9 The Company has taken steps to prevent its services from being accessed by individuals located in countries in the list of 'high risk third countries' identified by the European Commission.

Products, services, transaction and delivery channel risk factors

4.10 The services the Company provides are, by their nature, potentially attractive to money launderers as a means of placing, layering, or integrating laundered funds in the UK. The services offered by the Company allow customers to covert assets which have potentially been acquired illegally or through use of criminal proceeds into what is equivalent to fiat currency, and then to use that to purchase assets and/or services, thereby adding another layer of transactions. It also allows the value inherent in the crypto-assets to be transferred to a third party under the guise of a legitimate commercial transaction. This factor is supplemented by the fact that crypto-assets, by their nature, have very limited data available regarding their specific origination and the parties involved in their generation. This therefore substantially limits the Company's ability to trace the source of the assets and obtain evidence of their legitimate origins.

4.11 Additionally, as this business operates solely online, there is therefore no face-to-face interaction with customers. This increases the difficulty in verifying the identity of customers, and the risk of impersonation/fraud.

4.12 This being said, as the ultimate transactions must be connected to previously approved merchants, there are therefore substantive limitations on where the value inherent in the crypto assets can be transferred to. This does reduce the likelihood of the Company being used to facilitate financial crime to an extent, albeit not completely given the Company could still be used for integration/extraction of value purposes.

4.13 Taken together, these factors suggest the risk of the Company' business specifically being used for money laundering or terrorist financing purposes is moderate.

5. TRANSACTIONS WITH LINKS TO "HIGH RISK THIRD COUNTRIES"

5.1 It is the Company's policy not to enter into any transaction or arrangement with links to certain countries which are identified as 'high risk third countries' by the European Commission, without prior written permission from the CO so as to manage its financial crime risk. The current list of high risk countries is: Afghanistan, Bosnia and Herzegovina, Guyana, Iraq, Lao PDR, Syria, Uganda, Vanuatu, Yemen, Ethiopia, Sri Lanka, Trinidad and Tobago, Tunisia, Pakistan, Iran, and North Korea. A consolidated version of the list of high risk third countries is available on the European Commission website here. Transactions/arrangements with links to such countries (for example because a prospective investor is a resident of, or established in, one of them) should be regarded as presenting a high risk of money laundering and terrorist financing.

6. THE COMPLIANCE OFFICER ("CO")

6.1 Under POCA 2002 the Company is required to have a 'nominated officer' to receive reports of knowledge and/or suspicion of money laundering. The Company refers to the individual performing this role as the CO. That person is Arianny Viviana Seijo Noguera and will receive reports of suspected money laundering from Company employees.

6.2 The CO will also provide advice on anti-money laundering and terrorist financing issues to Company employees, and should be the first point of contact for Company employees who have concerns about either of these issues, or who need to make a money laundering report, even if they do not work within the regulated parts of the Company's business.

7. UNDERSTANDING THE KEY UK MONEY LAUNDERING OFFENCES

What is "criminal property"?

7.1 In the UK, the main offences of money laundering are contained in POCA 2002. They apply to the Company and all Company employees (not just Regulated Sector Employees). They depend upon the key concept of "criminal property". This is defined very widely.

7.2 "Criminal property" is any benefit (monetary or otherwise) from "criminal conduct", or any property representing the same (in whole or in part, and whether directly or indirectly), provided the alleged offender knows or suspects the property is or represents such a benefit.

7.3 "Criminal conduct" is conduct which:

7.3.1 constitutes an offence in the UK (for example fraud, bribery, or theft); or

7.3.2 would constitute an offence in the UK if it happened there.

7.4 It does not matter:

7.4.1 who carried out the criminal conduct; or

7.4.2 who benefited from it; or

7.4.3 how old it is.

7.5 In the context of the Company's business, by way of example:

7.5.1 Investments acquired by an individual who paid the Company using the proceeds of a fraud in the UK could constitute "criminal property";

7.5.2 Similarly, shares where an investor has paid partly from a legitimate source, and partly using criminal property from a fraud in the UK, could also constitute "criminal property"; and

7.5.3 The Company processing a purchase or sale of shares could involve a transfer of "criminal property" to the Company (the property itself, or the proceeds of the sale).

Criminal conduct that took place overseas

7.6 Company employees must not assume that overseas conduct cannot give rise to "criminal property" in the UK, or a UK money laundering offence. This is not the case. Subject to certain limited exceptions, handling the proceeds of a crime committed overseas can constitute money laundering in the UK.

The substantive money laundering offences in POCA 2002

7.7 The principal money laundering offences in POCA 2002 are very wide, and in practice cover most activity related to "criminal property". The offences are:

7.7.1 s327 POCA 2002: An offence is committed if a person conceals, disguises, converts, transfers or removes criminal property from England and Wales.

7.7.2 s328 POCA 2002: An offence is committed when a person enters into or becomes concerned in an arrangement which he knows or suspects will facilitate another person to acquire, retain, use or control criminal property.

7.7.3 s329 POCA 2002: An offence is committed when a person acquires, uses or has possession of criminal property.

7.8 In the context of the Company's business, by way of example, a transaction whereby a customer is selling crypto-assets where it is known or suspected that the customer is used "criminal property" to pay for those crypto-assets could potentially involve commission of all of the offences above:

7.8.1 the s327 offence could be committed by the investor - as "criminal property" would be transferred from one form to another when the crypto-assets are sold in exchange for the balance of fiat currency;

7.8.2 the s328 offence could be committed by the Company through processing the transaction – the processing of the generation of the fiat currency balance would likely be regarded as an "arrangement" that facilitated the customer's retention or use of criminal property;

7.8.3 the s329 offence could potentially be committed by the Company receiving the crypto-assets and therefore acquired, used or possessed 'criminal property'.

Penalties

7.9 The money laundering offences in POCA 2002 are very serious and can be prosecuted before a criminal court. **The maximum penalty for commission of any of them is 14 years' imprisonment, an unlimited fine, or both.**

Avoiding commission of the offences

7.10 The principal way to prevent the Company's business being used for money laundering (and therefore to avoid a Company employee risking the commission of an offence) is:

7.10.1 for due diligence to be carried out on each customer at a risk appropriate level so that actual or suspected attempts to use the Company's services for financial crime can be immediately identified;

7.10.2 for transaction monitoring to be undertaken to identify where a transaction is suspicious in light of the data the Company holds and may therefore require additional customer due diligence to be performed;

7.10.3 for employees to make a report to the CO as soon as possible, in the way explained later in this policy; and

7.10.4 where there is knowledge or suspicion of financial crime, for transaction which are outside of the Company's risk appetite to be rejected.

7.11 The CO is subject to a specific statutory offence which states that where:

7.11.1 they know or suspect that someone is engaged in money laundering;

7.11.2 the information or other matter on which their knowledge or suspicion is based came to them in consequence of a disclosure made by an employee of knowledge/suspicion of money laundering; and

7.11.3 knows or can identify (from the information they hold) the person doing the money laundering or the whereabouts of the laundered property as a consequence of the disclosure; or

7.11.4 has information which they believe, or it is reasonable to expect them to believe, will or may assist in identifying the person doing the money laundering or the whereabouts of the laundered property

then they must make a disclosure to the NCA about the matter.

7.12 **Failure to do so is a serious offence in its own right for the CO. The maximum penalty for commission of it is 5 years' imprisonment, an unlimited fine, or both. The Company expects all employees to assist the CO in complying with their duties in respect of preventing the risk of the Company being used for the purposes of financial crime.**

8. TERRORIST FINANCING

8.1 The Company's Risk Assessment assess its exposure to terrorist financing as moderate. Company employees must note the following key points:

8.1.1 part 3 of TA 2000 contains a series of criminal offences which make it illegal to fund terrorism and to use or possess "terrorist property". These apply in addition to the money laundering offences set out above;

8.1.2 "terrorist property" is defined widely to include: (a) money or other property which is likely to be used for the purposes of terrorism; (b) proceeds of the commission of acts of terrorism, and (c) proceeds of acts carried out for the purposes of terrorism. It could potentially include Company property;

8.1.3 part 3 TA 2000 requires the Company and Company employees to report suspicions of terrorist activity or dealings in "terrorist property";

if any Company employee has any concerns whatsoever that the Company's activities could in any way be linked to terrorism or the funding of terrorism, that is a matter of utmost seriousness. The individual concerned must approach the CO immediately to report the matter and seek further advice. The CO may seek specific legal advice as required.

9. FINANCIAL CRIME

9.1 The Company has certain obligations to its customers, and under UK law, to prevent its services from being used for the purposes of a wider range of financial crimes than just money laundering – for example, the Company should not allow its services to be used to commit fraud on third parties.

9.2 Where the Company and its services are used as an accessory for a financial crime, in addition to the Company potentially breaching its obligations to its clients and under UK law, the proceeds from the wider financial crimes are very likely to fall within the definition of 'criminal property' for the purposes of the money laundering regime.

9.3 Given the Company is involved in the arrangements relating to the completion of transactions with merchants, there is a risk that the merchants who ultimately receive the funds may be misrepresenting their identity, activities and/or financial position, and/or may misappropriate the funds they receive. The Company has an obligation to mitigate this risk as much as possible.

9.4 Consequently, the Company has incorporated elements into its procedures that will allow it to consider the risk that it may be used for fraudulent purposes by a merchant, and will assess the validity of applications to join the Company's services in a similar manner to the CDD carried out on customers seeking to exchange crypto-assets.

10. AML REQUIREMENTS OF ALL COMPANY EMPLOYEES

Day to day activities

10.1 Company employees must not, without the consent of the CO (or an authority such as the National Crime Agency ("NCA"), as appropriate):

10.1.1 put him or herself, or the Company, at risk of committing one of the money laundering offences set out above;

10.1.2 handle or deal with any property that is "criminal property", including:

(a) accepting or making assets suspected to be "criminal property";

(b) agreeing to enter into transactions or other arrangements that are known or suspected to involve "criminal property";

10.1.3 attempt to handle "criminal property";

10.1.4 agree with anyone to handle "criminal property";

10.1.5 encourage or assist someone else to handle "criminal property";

10.1.6 disclose to anyone else the fact that they have approached the CO about a potential money laundering issue;

10.1.7 disclose to anyone else the fact that a Suspicious Activity Report ("SAR") has been made to the CO or to the authorities;

10.1.8 disclose to anyone else the fact that a money laundering investigation is being contemplated or carried out;

10.1.9 make any disclosure that might prejudice a money laundering investigation; or

10.1.10 falsify, conceal, destroy or otherwise dispose of (or cause the falsification, concealment, destruction or disposal of) documents likely to be relevant to a money laundering investigation.

10.2 Doing any of the above could constitute a criminal offence by the Company employee and potentially by the Company.

10.3 Any Company employee who knows or suspects that anyone (in any capacity: an individual investor, an employee of a corporate investor, a party seeking investment) is or may be involved in using the Company's business for money laundering must:

10.3.1 contact the CO immediately to seek advice and, if appropriate, report the matter. Do not delay, as to do so may make it impossible for the individual concerned, and the Company, to obtain a defence to a money laundering offence;

10.3.2 keep good records of the information that has caused them to become concerned, e.g. any notes made during a meeting or call with an occupier, lawyer or agent where relevant information is discussed;

10.3.3 obey any instructions given by the CO with respect to the matter, including any instruction not to proceed with the relevant activity or transaction that may involve money laundering until consent has been granted by the authorities.

Procedures for dealing with suspicions of money laundering

10.4 From time to time:

10.4.1 professional services firms advising the Company (such as solicitors or agents) may raise potential money laundering issues with the Company in a transactional context; and/or

10.4.2 a Company employee may, through the course of assisting with a transaction, develop his or her own knowledge or a suspicion of money laundering.

10.5 In such circumstances:

10.5.1 the general requirements for AML risk management set out in this policy continue to apply, in particular the Company employee(s) concerned must contact the CO immediately to make a report and must not to disclose to others (including other parties to the transaction) the fact that a report has been made unless the CO authorises this;

10.5.2 it may be necessary for the CO to obtain the authorities' consent for the transaction to proceed, without informing any other party to the transaction (or allowing others to do so). Company employees must obey instructions from the CO in that regard;

10.5.3 if the Company has instructed professional advisers (for example any solicitors or agents), it is likely that those advisers will have their own obligations to make reports to the authorities. Advisers' concerns may or may not be disclosed to the Company. Company employees should, at the time that they make their own report, be ready to give the CO details of any such firms or individuals who are advising the Company. In some cases, a joint report by the Company and its advisers may be advisable or appropriate. However, communication about potential money laundering issues with anyone outside of the Company is restricted by law and should be in practice led by the CO or done only with the CO's consent.

11. CUSTOMER DUE DILIGENCE OBLIGATIONS ON THE COMPANY

11.1 In order to manage its financial crime risk, the Company applies customer due diligence measures when it:

11.1.1 establishes a business relationship with a "customer" (e.g. when it accepts an application to open an account for the exchange of crypto-assets for an individual/corporate client);

11.1.2 suspects money laundering, terrorist financing or fraudulent behaviour, for example where a transaction is unusually large and/or there is an unusual pattern of transactions; or

11.1.3 doubts the veracity or adequacy of documents or information previously obtained from its customers for the purposes of identifying them.

11.2 A "customer" of the Company in these circumstances means a person with whom the Company has a business, professional or commercial relationship. In practice, "customers" of the Company are likely to be (i) individuals or corporates wishing to exchange crypto-assets with the Company for a fiat currency balance; and (ii) merchants willing to accept the fiat currency balances as a means of payment.

11.3 In these circumstances, the Company must:

11.3.1 identify the customer;

11.3.2 "verify" the customer's identity (in the sense of using documents obtained from a reliable source independent of the person whose identity is being verified, such as the public register of companies held at Companies House); and

11.3.3 assess and, where appropriate, obtain information on the purpose and intended nature of the business relationship or occasional transaction (typically, why the customer requires insurance, what the Company will be expected to do in that regard and how often).

11.4 Where the customer is a company, the Company is required to:

11.4.1 obtain its name and company or other registration number; and

11.4.2 the address of its office and (if different) the principal place of its business.

11.5 Unless the customer is listed on a regulated market, the Company is also required to:

11.5.1 take reasonable measures to determine and verify the law to which the company is subject, and its constitution;

11.5.2 the full names of its board of directors and the senior person responsible for its operations;

11.5.3 where it is beneficially owned by another person, identify the beneficial owner and take reasonable measures to verify the identity of the beneficial owner so the Company is satisfied it knows who the beneficial owner is;

11.5.4 where the beneficial owner is a company (as will usually be the case), take reasonable measures to understand its ownership and control structure; and

11.5.5 keep written records of the actions taken to identify the beneficial owner.

11.6 This information may be available publicly at Companies House, or through normal due diligence procedures.

11.7 The Company will need to obtain documentation in line with its CDD procedures, before permitting a customer to use its services, or allowing a merchant to carry out transactions facilitated by its services. In any case that is considered to present a higher risk of money laundering, more detailed ('enhanced') due diligence on the "customer" may be required. The

Company should consult the CO (and may wish to take separate legal advice) in any cases which appear to be higher risk.

11.8 In addition to the above:

11.8.1 As identified in the Company's AML Risk Assessment, different customers/merchants may involve different levels of money laundering risk depending in particular upon the crypto-asset in question, the countries/geographies involved, and the various corporate structures of the parties involved. Whilst the Company utilises standardised procedures to carry out CDD, the Company recognises that there is not a 'one-size fits all' approach to CDD, and may therefore alter the level of CDD carried out on a customer and/or how this CDD is carried out, depending on the specific circumstances of the situation.

11.8.2 Where adverse information comes to light during the due diligence process that cannot be addressed satisfactorily, the Company will not proceed with letting the relevant entity have access to its services. Suspicions arising from information discovered during due diligence should be reported to the CO as set out above;

11.8.3 in all cases, regardless of any other due diligence being done, the Company will obtain a report (which includes checks for politically exposed persons ("PEPs") and sanctions screening checks) on potential customers at an early stage, to identify whether or not any PEPs are involved, and confirm that it would not be dealing with an individual or entity subject to UK, EU, US or UN sanctions. The Company will automatically refuse any application where the customer (or a beneficial owner of the customer) is a PEP. Furthermore, typically, dealing with the subject of a financial sanction or assisting a person to circumvent a financial sanction will involve commission of a criminal offence in the UK. As a result, if the report identifies a potential sanctions match, it must be reviewed and approved by the CO before access can be granted can proceed;

11.8.4 some types of adverse information detailed in the report may be addressed satisfactorily by making further inquiries of the customer as part of the due diligence process. For example, the Company may be able to address concerns by confirming the occupier's source of wealth and that a legitimate source of funds will be used to meet obligations under the lease;

11.8.5 a review of the PEP list will be conducted quarterly to assess if any current customers have become a PEP since first being approved; and

11.8.6 if suspicions or concerns arise after access has been granted, the Company may nevertheless be under reporting obligations and will seek legal advice as appropriate. If, following completion of an exchange via the Company's services, an alert with adverse information in it relating to one of the transaction parties is generated, this alert must be escalated to the CO without delay. Further, if a Company employee becomes aware of adverse media coverage or other information about a customer and/or a transaction that suggests there may be a money laundering issue, this should also be drawn to the CO's attention.

12. TIMING OF CUSTOMER DUE DILIGENCE

12.1 The Company must normally carry out due diligence when it establishes the business relationship with the "customer". However, it must also apply customer due diligence measures at other appropriate times, taking a risk based approach, in particular where it appears the customer's

identity or ownership has changed, the relationship is not being used as intended, or there appears to be a risk of money laundering.

12.2 Where the Company is unable to apply customer due diligence measures, it must:

12.2.1 not establish a business relationship with the customer (if applicable);

12.2.2 not accept crypto-assets from the customer;

12.2.3 must terminate any existing business relationship (if applicable);

12.2.4 review any historic transactions to determine if these presented a risk of involvement in financial crime; and

12.2.5 must consider whether it is required to make a report to the CO.

13. ONGOING MONITORING OF THE BUSINESS RELATIONSHIP

13.1 The Company conducts ongoing monitoring of business relationships to ensure that they are being used as originally intended and consistently with the Company' knowledge of the customer and the purpose for which the relationship was to be used.

13.2 In the normal course of business, the Company should be able to discharge its obligation to carry out ongoing monitoring through a variety of compliance-related tasks, including capturing data, filtering, recordkeeping, investigation management, and reporting.

13.3 System functionalities include:

13.3.1 Daily check of customers on the presence in the recognized "black lists" (e.g. OFAC),

13.3.2 placing Users on watch and service denial lists as appropriate, and

13.3.3 CDD information and document reviews (both ad hoc and periodic).

13.4 In addition to reviews of CCD, the Company will be engaged in transaction monitoring activities. The Company will engage in analysis of customer transaction patterns through data analysis and suspicious activity detection tools to assess if particular transactions are outside either the general trends/risk profile the Company has established (by aggregating transfers by multiple data points) and/or the typical approach taken by the specific customers.

13.5 Where a transaction presents as potentially being of a higher risk of financial crime based on the above monitoring, the Company will carry out appropriate further investigations to determine if there is financial crime present, or grounds for suspicion of financial crime. This may result in a report to the CO.

13.6 To further mitigate risks, the Company imposes transaction value thresholds whereby customers who wish to carry out higher value exchanges must be subject to higher levels of CDD so as to reflect the increased risk of financial crime. Such thresholds operate of cumulative and individual transaction assessments so as to decrease the likelihood of smurfing allowing transactions/customers avoid additional CDD.

14. RECORD KEEPING

14.1 There are minimum record keeping requirements for due diligence carried out for AML purposes. The Company must keep records of any documents that it has obtained as part of the due diligence it has carried out on customers for 5 years, beginning on the date on which it has reasonable grounds to believe that the transaction or business relationship has come to an end - Please see the Company's retention policy for further information.

15. TRAINING OF STAFF

15.1 The Company carries out specific AML, CTF and financial crime training as part of its employee onboarding process, and it is mandatory for all employees to undertake refresher training on these subjects on an ongoing basis.

15.2 The training programme is the responsibility of the CO who, with appropriate external advice and support ensures the following:

Content	- The UK's statutory and regulatory regime in relation to financial crime. - The specific offences that can be committed by various employees within the business. - The role of the CO. - The financial crime risks that the business is exposed to and how the Company looks to mitigate and manage these. - The CDD and SAR procedures the Company has in place, as well as wider employee obligations in respect of combating financial crime.
Recipients	- All directors, senior managers and employees - Consultants, secondees and similar workers will be determined on a case-by-case basis
Frequency	- All employees will receive training as part of their onboarding as employees. - At a defined point annually, all employees will complete a refresher training session.
Delivery method	- Desk-based training slides, accessible at employee's discretion
Confirmation	- Each time an employee receives training, they will be required to complete a mandatory assessment. They must pass this assessment in order to complete the training. - As part of an individual's annual performance review, it will be confirmed if the individual completed that year's financial crime training. Additionally, automated systems will identify to the CO those who have not completed the annual training within 1 month of the training programme going live.

16. PROCEDURES FOR DEALING WITH AML-RELATED REQUESTS ABOUT THE COMPANY FROM OTHER PARTIES

16.1 Some providers of professional services to the Company (in particular banks and other financial institutions, solicitors, and agents) will be under AML obligations to carry out 'know your client' on the Company as their customer. The key obligation imposed upon them by the MLRs 2017 is to confirm and verify the identity of their customer and usually they must do this before they can provide their services. Similarly, from time to time, professional services firms acting for other

parties (for example solicitors acting for an investor) will be under an obligation to carry out KYC on the Company as one of the other parties to the arrangements (for example, where the platform is used to purchase investments issued by an entity and the Company remits the completion funds to the entity).

16.2 Whilst a search of Companies House will enable third parties to identify and verify key information such as the Company's name, registration number and registered office address, the MLRs 2017 require firms to take a risk-based approach. This means that the Company may receive requests for additional information beyond what is contained within public registers – particularly where the transaction triggering the requirement to carry out KYC on the Company presents indicators of there being a higher risk of money laundering. Where this occurs, Company employees should ask the person making the request to explain and justify the basis for the request, and then requests should be considered case by case.

KYC PROCEDURES

This procedure describes the process by which the Company carries out client due diligence on prospective customers/merchants prior to them being given access to the services. The same procedure is used for when an existing customer changes their relationship with the Company (for example, if they start engaging in a wider range of crypto-currencies, or place significantly more funds onto the platform). The purpose of this procedure is to help the Company to develop business that is within its commercial risk appetite, but also to ensure that it discharges its obligations with respect to customer due diligence that arise under UK anti-money laundering legislation and prevents its services being used for the purposes of other financial crimes.

1. STEP 1 – IDENTIFYING THE CUSTOMER AND DEFINING THE BUSINESS CASE

This stage is very important as it lays the foundation upon which the KYC procedure will be based. The process followed will differ depending on how the client will be using the platform.

Merchants

1.1 This stage consists of gathering as much information as possible from the merchant and reviewing it to fully understand the client's business proposition.

1.2 During this stage the information gathered from the client should address the following questions:

1.2.1 In which country is the merchant registered, and what is the merchant's name? Who are the merchant's directors, senior managers, shareholders etc.?

1.2.2 What currencies would they like to receive settlements?

1.2.3 Where is the merchant's bank account (which bank and in which country)?

1.2.4 What are they selling? What is the product/service and to which industry does it belong? Who are their typical customers?

1.2.5 What are their target markets/main regions where clients come from?

1.2.6 Do they need a license to operate? Is there a license? If yes, who issued it and when?

1.2.7 For how long have they been active?

1.2.8 Any additional information we should have?

1.3 This stage needs to be well documented internally so as to comply with, and evidence said compliance, with the UK AML requirements, as well as identifying a risk that the prospective client may use the platform for fraudulent purposes. The answers to these questions should be documented and entered into the Company's records on the potential client.

Exchange customer

1.4 This stage consists of gathering as much information as appropriate and possible from the customer so that the Company is clear on who the customer is holding themselves out to be, so that this can be verified against documentary evidence.

1.5 During this stage the information gathered from the client should address the following questions:

1.5.1 Who is the actual customer (i.e. private individual, company, trust etc.)? What is the relationship of the person completing the identification information to the entity investing?

1.5.2 If the entity is a company, in which country is the company registered, and what is the company's name? Who are the company's directors, senior managers, shareholders etc.?

1.5.3 If the entity is an individual, what is their name, what is their date of birth and where are they resident?

1.5.4 If a trust, who are the beneficiaries, trustees etc.?

1.5.5 What crypto-assets are they intending to exchange?

1.5.6 What volume of transactions are they intending to carry out?

1.5.7 What merchants are they intending to use?

1.5.8 Any additional information we should have?

1.6 This stage needs to be well documented internally so as to comply with, and evidence said compliance, with the UK AML requirements, as well as identifying a risk that the prospective client may use the platform for fraudulent purposes. The answers to these questions should be documented and entered into the Company's records on the potential client.

2. STEP 2 – DOCUMENT COLLECTION

2.1 Each customer (regardless of how they will use the services), if they are an incorporated entity, will need to provide the following documents for review:

2.1.1 Certificate of incorporation

2.1.2 Memorandum and articles of association

2.1.3 Identities of Beneficial Owners (who may be subject to CDD as though they were the direct customer, based upon their risk profile)

2.1.4 Identities of the directors (or equivalent) (who may be subject to CDD as though they were the direct customer, based upon their risk profile).

These documents must be certified by a lawyer, accountant, notary public or Consular Official at the British Embassy or Consulate.

Merchants

2.2 In addition to the documents specified at paragraph 2.1, the Company will require documents issued by a regulated third party providing proof of business address (e.g. utility bills for the property/extracts from company registers).

2.3 The Company also requires that all sole traders, partners and any Beneficial Owners of a merchant (as applicable) and, where the merchant is an incorporated company, at least two directors of the merchant provide verification evidence fulfilling each of the categories detailed in the table in paragraph 2.4

Exchange customer (and beneficial owners/directors where relevant)

2.4 A risk-proportionate approach is taken to verification of exchange customers. Depending on the volume of transactions they intend to or are carrying out, additional levels of verification may be performed. The following table shows how this is implemented:

Verification being sought	Customers it applies to	Accepted evidence	Method of collection
Name and date of birth	All customers	ID document (e.g. colour copies of passport)	Scan from customer
Proof of residence	• Customers who intend to or have exceeded $100 in daily transactions in any one day. • Customers to who intend to or have exceeded $1,000 in monthly transactions in any one month. • Customers presenting a moderate financial crime risk	Utility bills or similar documents (not older than 3 months).	Scan from customer
Biometric data	• Customers who intend to or have exceeded $1,000 in daily transactions in any one day. • Customers to who intend to or have exceeded $5,000 in monthly transactions in any one month. • Customers presenting a higher financial crime risk	Picture of customer	Photo and facial scan captured through the exchange customer's device using the Company's app

2.5 As detailed above, depending on the particular level of transactions an exchange customer performs, they will be subject to additional levels of due diligence due to the increased financial crime risk larger volumes of transactions represent. The Company's systems automatically monitor a customer's transaction volumes on an ongoing basis. When a customer reaches the transaction value limit of their current verification level, the Company's systems will immediately suspend that customer's ability to perform further transactions until they complete the requirements for the next level of verification. The customer will receive a notification advising them of the need to submit additional CDD information and the implications of not doing this. Following the customer's submission of the additional requested data, and the Company confirming that it meets its requirements for the additional CDD, the customer's functionality will be reinstated.

3. REVIEW

3.1 During the review of the verification information, a member of the compliance team:

3.1.1 reviews the adequacy of the documentary evidence received;

3.1.2 compares the documentation received against the information gathered from the customer; and

3.1.3 obtains a report which includes checks for politically exposed persons ("PEPs") and sanctions screening and any other relevant individuals named as part of the information gathering.

3.2 Any discrepancies/immediate issues are highlighted and brought to the attention of the CO. Such escalation may result in:

3.2.1 a risk of money laundering/financial crime being identified, and the relevant notification processes being engaged;

3.2.2 an identification that the enhanced due diligence or further information on the customer is required, in which case advice will be sought on the additional verification steps that should be undertaken; or

3.2.3 the current documentation and information being deemed suitable, and therefore the standard due diligence process will be continued.

3.3 Furthermore, any documentation that doesn't conform to the Company's standards or is missing is grounds for rejection of the application.

3.4 As part of the process described in paragraph 3.1 above, the following checks will be performed:

Document Authentication Check and PEP/Sanction List Check

3.5 Staff members responsible for performing CDD on any type of client will, in all cases, be required to submit details regarding:

3.5.1 their identity (e.g. full name, date of birth, address); and

3.5.2 documents gathered for verification purposes (e.g. passport number),

into the integrated platform provided by the third party service provider the Company uses to assist with additional identification/verification actions.

3.6 Where this platform returns a result which indicates:

3.6.1 one or more of the documents the client has provided are, or may be, false, inaccurate and/or incomplete; and/or

3.6.2 the client appears on a PEP/sanction list,

the staff member should:

3.6.3 review the results to confirm if it is a clear false positive result or if there was a flaw in the initial data the staff member input;

3.6.4 if it is not an obvious false positive result and all data was input correctly, this result should be escalated in accordance with paragraph 3.2.

Reputational Check

3.7 Google checks are performed on all companies and individuals that appear in the company documents as well as the website. Key words are used to find negative results such as scam, fraud etc.

3.8 During this check, the reviewer must consider:

3.8.1 For merchants - how long the brand or company has been in existence (and verify that no results are found from before these dates) and whether there is an indication of PEP involvement. Furthermore, adverse media of any type will also be considered.

3.8.2 For exchange customers/beneficial owners/directors – whether there are any indications that the customer is or may be involved with PEPs. Furthermore, adverse media of any type will also be considered.

3.9 Any negative results found are brought are escalated and a decision made if these would prevent the Company on-boarding the customer and/or if they need to be discussed with the customer.

4. REVIEW AND APPROVAL

4.1 It is the policy of the Company not to provide access to the services to, accept assets from, or carry out any transactions of any kind in respect of, any customer until (i) that customer has provided documentation to required standards set out above, (ii) the customer's identity has been verified to a suitable level according to their risk profile, and (iii) the customer has accepted the relevant terms of business.

4.2 In the event that the KYC process described above is carried out as repeat KYC for an existing customer (for example because a suspicion has arisen during the course of a relationship, or because information has come to light that the customer's original risk profile has changed), and the customer is not able to provide documentation to the required standard, the Company will terminate its existing business relationship and consider whether a disclosure is required to the UK authorities.