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

1. POLITICS

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

0. COMPLIANCE

2.1 All Company employees are expected to become familiar with and comply with this policy.

2.2 Strict compliance with the provisions of this policy and other anti-money laundering and anti-terrorist financing regulations 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 may also expose the individual concerned to the risk of criminal prosecution. In particular, failure to report known or suspected money laundering to the Compliance Officer ("CO") is likely to be a criminal offence, and is considered a serious misconduct which may result in immediate dismissal. without payment. The board of directors, with the assistance of the CO, is responsible for initiating and overseeing the investigation of all reports of violations of this policy and other regulations and for ensuring that appropriate disciplinary action is taken when necessary.

0. WHAT IS MONEY LAUNDERING?

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

3.2 "The objective 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 hide their illegal origin. This process is of vital importance, since it allows the criminal to enjoy these benefits without endangering their source..."

3.3 "When criminal activity generates substantial profits, the individual or group involved must find a way to control the funds without drawing attention to the underlying activity or the people 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 Money laundering typically occurs in several stages.

3.4.1 First of all, in the initial stage -or placement-, the launderer introduces his illegal profits into the financial system. This could be done by dividing large amounts of cash into smaller, less visible sums which are then deposited directly into a bank account, or by

purchasing a series of monetary instruments. (checks, money orders, etc.) that are then collected and deposited into accounts elsewhere.

Second, after the funds have entered the financial system, a layering phase 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 could be channeled through the buying and selling of investment instruments, or the launderer could simply transfer the funds through a series of accounts at various banks around the world. This use of widely dispersed accounts for laundering is especially prevalent in those jurisdictions that do not cooperate in anti-money laundering investigations. In some cases, the launderer may disguise the transfers as payments for goods or services, thus giving them a legitimate appearance.

3.4.2 Third, having successfully processed the criminal proceeds through the first two phases, the launderer moves them to the third phase, integration, in which the funds re-enter the legitimate economy. The launderer could choose to invest the funds in real estate, luxury assets or companies.

3.5 The Company, through its acceptance of cryptocurrencies in exchange for electronically stored balances of fiat currency that can be used to purchase goods and services, is particularly exposed to second and third stage money laundering.

0. RISKS EVALUATION

4.1 In accordance with industry guidance, the Company understands that its anti-money laundering and anti-financial crime measures should be commensurate with the level of risk, and designed to mitigate and manage the specific risks inherent in both its business and transactions. in which it is involved. To this end, 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 evaluation is carried out on an ongoing basis and is updated as appropriate based on changes in the business and its operations. A summary of current risk assessments is as follows:

Overall risk assessment

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

4.4 The Company's activities that are exposed to the highest risk of financial crime are the core business and are carried out on a routine and high-volume basis. While the Company does not receive cash from customers, it does receive assets that may have been purchased using criminal property, then converts those assets into monetary value that can be exchanged for goods and services. 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 to third parties. The relative degree of anonymity involved in cryptocurrencies, as well as the fact that cryptocurrencies are not tied to specific jurisdictions and the distribution channels used, increases the risk factors for the Company.

Client risk factors

The clients of the Company's services are mainly restricted, in practice, to individuals, but there are certain corporate clients. Clients can potentially be based in any location and are not restricted in their regulatory classification (i.e. the Company could deal with retail consumers conducting one-off trades as well as professional cryptocurrencies users conducting regular trades). As cryptocurrencies re not a common investment asset, and trying to convert them into fiat currency is not a typical service, it is unlikely that the Company's clients could be viewed as having an equivalent risk profile to other e-money and remittance users. of money.

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

4.6 Another potential risk is that the Company does not have ongoing customer relationships, with some customers potentially engaging in one-time transactions with the Company. Therefore, this limits the Company's opportunity to collect a range of data about the customer and their transactions to help identify suspicious trends. This is somewhat mitigated by the fact that the exchanges will be directly related to purchasing power as specific merchants, thus giving a clear picture of who the value of the crypto assets will ultimately be transferred to, although it does not fully mitigate the risk.

Countries and geographic risk factors

4.7 The Company's activities may have links to high-risk jurisdictions. The Company itself conducts business in the UK, although clients and transferred assets may originate from jurisdictions outside the UK and EEA. Therefore, the Company is directly exposed to foreign jurisdictions (including members that are not members of the FATF).

4.8 The Company has taken measures to prevent its services from being accessed by persons located in countries on the list of "high risk third countries" identified by the European Commission.

Risk factors of products, services, transactions and delivery channels

4.9 The services offered by the Company 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 clients to conceal assets that have potentially been acquired illegally or through the use of criminal proceeds in what is equivalent to fiat currency, and then use them to purchase assets and/or services, thus adding another layer of transactions. It also allows the value inherent in cryptocurrencies to be transferred to a third party under the guise of a legitimate business transaction. This factor is complemented by the fact that cryptocurrencies, by their nature, have very limited data available regarding their specific origin and the parties involved in their generation. Therefore, this substantially limits the Company's ability to trace the source of the assets and obtain evidence of their legitimate origins.

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

4.11 That said, as final transactions must be connected to pre-approved merchants, there are therefore substantive limitations on where the value inherent in cryptocurrencies can be transferred. This reduces the likelihood that the Company will be used to facilitate financial crime to some extent, though not completely as the Company could still be used for value integration/extraction purposes.

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

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

5.1 The Company's policy is not to enter into any transactions or agreements that have any link to certain countries that the European Commission identifies as "high risk third countries" without the prior written permission of the CO to manage your 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 those countries (for example, because a potential investor is a resident of one of them or established in one of them) should be viewed as a high risk for money laundering and terrorist financing.

0. THE COMPLIANCE OFFICER ("CO")

6.1 Under POCA 2002, the Company is required to have an "appointed officer" to receive reports of known and/or suspected money laundering. The Company refers to the person performing this role as the CO. That person will receive reports of suspected money laundering from Company employees.

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

0. UNDERSTAND THE UK'S MAIN MONEY LAUNDERING CRIMES

What is "criminal property"?

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

7.2 "Criminal property" is any profit (monetary or otherwise) obtained from "criminal conduct", or any property representing the same (in whole or in part, and whether directly or

indirectly), provided that the alleged criminal knows or suspects that the property is or represents such a benefit.

7.3 "Criminal conduct" is conduct that:

7.3.1 constitutes a crime in the UK (for example, fraud, bribery or theft); Eiter

7.3.2 it would constitute an offense in the UK if it occurred there.

7.4 Does not matter:

7.4.1 who carried out the criminal conduct; either

7.4.2 who benefited from it; either

7.4.3 When did it happen.

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

7.5.1 Investments purchased by a person who paid the Company using UK fraud proceeds could constitute "criminal property";

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

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

Criminal conduct that took place abroad

7.6 Company employees should not assume that conduct abroad may not give rise to "criminal property" in the UK, or a UK money laundering offence. This is not the case. Subject to certain limited exceptions, dealing with the proceeds of a crime committed abroad may constitute money laundering in the UK.

The substantive crimes of money laundering in the POCA of 2002

7.7 The main money laundering offenses in POCA 2002 are very broad and, in practice, cover most activities related to "criminal property". The crimes are:

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

7.7.2 s328 POCA 2002: An offense is committed when a person enters into or becomes involved in an arrangement knowing or suspecting that it will facilitate another person to acquire, retain, use or control criminal property.

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

7.8 In the context of the Company's business, for example, a transaction where a customer is selling cryptocurrencies when the customer is known or suspected to have used "criminal property" to pay for those cryptocurrencies could potentially involve the commission of all of the above crimes:

7.8.1 the s327 offense could be committed by the investor – as “criminal ownership” would be transferred from one form to another when the crypto assets are sold in exchange for the fiat currency balance;

7.8.2 s328 offense could be committed by the Company through the processing of the transaction – the process of generating the fiat currency balance would likely be considered an “agreement” that facilitated the retention or use of criminal property by the customer ;

7.8.3 the s329 offense could potentially be committed by the Company receiving the cryptocurrencies and thus acquired, used or possessed 'criminal property'.

Sanctions

7.9 The money laundering offenses in POCA 2002 are very serious and can be prosecuted in criminal court. The maximum penalty for committing either is 14 years in prison, an unlimited fine, or both.

Prevent the commission of crimes

7.10 The primary way to prevent Company business from being used for money laundering (and therefore to prevent a Company employee from committing a crime) is to:

7.10.1 conduct “Customer Due Diligence” (“CDD”) for each customer and according to their level of risk, so that actual or suspected attempts to use the Company's services for criminal offenses financial can be immediately identified;

7.10.2 conduct ongoing transaction monitoring to identify when a transaction is suspicious in light of the data the Company has and therefore may require additional customer CDD to be performed;

7.10.3 Employees make a report to the CO as soon as possible, in the manner explained later in this policy; and

7.10.4 when there is knowledge or suspicion of a financial crime, that the transactions that exceed the level of risk accepted by the Company are rejected.

7.11 The CO is subject to a specific legal statute that states that when:

7.11.1 knows or suspect that someone is involved in money laundering;

7.11.2 the information or other matter on which your knowledge or suspicion is based was obtained as a result of a disclosure by an employee of known/suspected money laundering; and

7.11.3 knows or can identify (from the information it has) the person doing the money laundering or the whereabouts of the laundered property as a result of the disclosure; either

7.11.4 have information that they believe, or can reasonably be expected to believe, will help to identify the person doing the money laundering or the whereabouts of the property laundered then they should make a disclosure to the ANC about the matter.

7.12 Failure to do so is a serious offense in its own right for the OC. The maximum penalty for committing the same is 5 years in prison, an unlimited fine, or both. The Company expects all employees to assist the CO in fulfilling his duties with respect to preventing the risk of the Company being used for the purposes of financial crime.

0. FINANCING OF TERRORISM

8.1 The Company's Risk Assessment assesses its exposure to terrorist financing as moderate. Employees of the company must take into account the following key points:

8.1.1 Part 3 of the TA 2000 contains a series of offenses that make it illegal to finance terrorism and to use or possess "terrorist property". In addition to the money laundering offenses set forth above;

8.1.2 "terrorist property" is broadly defined to include: (a) money or other property that can be used for terrorist purposes; (b) income from the commission of acts of terrorism and (c) income from acts carried out for the purpose of terrorism. Could potentially include Company property;

8.1.3 part 3 of the TA 2000 requires Company and Company employees to report suspected terrorist activities or dealings in "terrorist property";If any Company employee has any suspicion that the Company's activities may in any way be linked to terrorism or the financing of terrorism, that is a matter of the utmost seriousness. The interested party should immediately contact the CO to report the matter and request further advice. The CO may seek specific legal advice as needed.

0. FINANCIAL CRIMES

9.1 The Company has certain obligations to its clients, and under UK law, to prevent its services from being used for the purposes of a wider range of financial crimes than simple money laundering – for example, the Company must not allow its services are used to commit fraud against third parties.

9.2 Where the Company and its services are used as an accessory to a financial crime, as well as the Company potentially breaching its obligations to its clients and under UK law, the proceeds from these broader financial crimes are most likely to be listed as ' criminal property' for the purposes of the money laundering regime.

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

9.4 Accordingly, 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 requests to join the Company's services in a manner similar to the CDD carried out on clients looking to trade cryptocurrencies.

0. AML REQUIREMENTS OF ALL COMPANY EMPLOYEES

Daily 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 yourself, or the Company, at risk of committing one of the money laundering offenses set out above;

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

. accepting or processing property suspected of being "criminal property";

b. agree to enter into transactions or other arrangements known or suspected of involving "criminal property";

10.1.3 trying to handle "criminal property";
10.1.4 agreeing with any person to handle "criminal property";

10.1.5 encouraging or assisting another person to handle "criminal property";

10.1.6 disclose to any other person the fact that a potential money laundering problem has been reported to the CO;

10.1.7 disclose to any other person the fact that a Suspicious Activity Report ("SAR") has been made to the CO or to law enforcement;

10.1.8 disclose to any other person the fact that a money laundering investigation is being contemplated or carried out;

10.1.9 make any disclosure that could prejudice a money laundering investigation; either

10.1.10 falsifying, concealing, destroying or otherwise disposing of (or causing the falsification, concealment, destruction or elimination of) documents that may be relevant to a money laundering investigation.

10.2 Doing any of the foregoing could constitute a criminal offense by the Company employee and potentially by the Company.

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

10.3.1 contact the CO immediately for advice and, if appropriate, report the problem. You should not delay, as this may make it impossible for the individual concerned, and the Company, to obtain a defense to a money laundering offence;

10.3.2 keep a good record of the information that has caused them to be concerned, for example, any notes made during a meeting or call with an attorney or agent when relevant information is being discussed;

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

Procedures for dealing with suspicions of money laundering

10.4 Occasionally:

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

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

10.5 In such circumstances:

10.5.1 the general requirements for AML risk management set out in this policy still apply, in particular employees of the Company concerned must contact the CO immediately to make a report and must not disclose to others (including other parties to the transaction) the fact that a report has been submitted unless authorized by the CO;

10.5.2 It may be necessary for the CO to obtain the consent of the authorities for the transaction to take place, without informing any other party of the transaction (or allowing others to do so). The employees of the company must obey the instructions of the CO in this regard;

10.5.3 If the Company has instructed professional advisers (for example, any attorney or agent), those advisers may have their own reporting obligations to the authorities. Advisors' concerns may or may not be disclosed to the Company. Company employees should, at the time they make their own report, be ready to give details of the CO of such companies or individuals who are advising the Company. In some cases, a joint report by the Company and its advisors may be advisable or appropriate. However, communication about potential money laundering issues with anyone outside of the Company is restricted by law and should in practice be directed by the CO or made only with the consent of the CO.

11. CUSTOMER CDD OBLIGATIONS TO THE COMPANY

11.1 In order to manage its risk of financial crime, the Company applies CDD measures to the client when:

11.1.1 establish a business relationship with a "client" (for example, when you accept a request to open an account for the exchange of crypto assets for an individual/corporate client);

11.1.2 suspected money laundering, terrorist financing, or fraudulent behavior, for example, when a transaction is unusually large and/or there is an unusual pattern of transactions; either

11.1.3 doubts the veracity or adequacy of the documents or information previously obtained from its clients in order to identify them.

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

11.3 In these circumstances, the Company must:

11.3.1identify the customer;

11.3.2 "verify" the identity of the client (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 maintained by Companies House); and

11.3.3 assess and, where appropriate, obtain information about the purpose and intended nature of the occasional business relationship or transaction (typically why the customer wants to open an account, what the Company is expected to do about it and how often) .

11.4 When the client is a company, the Company is obliged to:

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

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

11.5 Unless the client appears on a regulated market, the Company is also obliged to:

11.5.1 take reasonable steps 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 of the person most responsible for its operations;

11.5.3 where beneficially owned by another person, identify the beneficial owner and take reasonable steps to verify the beneficial owner's identity to such a degree that the Company is satisfied that it knows who the beneficial owner is;

11.5.4 where the beneficial owner is a company (as is often the case), take reasonable steps to understand its ownership and control structure; and

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

11.6 This information may be publicly available at Company House, or through normal CDD procedures.

11.7 The Company will need to obtain documentation in line with its CDD procedures, before allowing a customer to use its services, or allowing a merchant to conduct transactions facilitated by its services. In any case deemed to present a higher risk of money laundering, a more detailed ('enhanced') CDD on the "customer" may be required. The Company should consult the CO (and may wish to take separate legal advice) in any case that appears to be of higher risk.

11.8 In addition to the above:

11.8.1 As identified in the Company's AML Risk Assessment, different clients/merchants may pose different levels of money laundering risk depending, in particular, on the crypto-asset in question, the countries/geographies involved, and the various corporate structures of the companies involved. parties involved. While the Company uses standardized procedures to conduct CDD, the Company recognizes that there is no "one size fits all" approach to CDD, and therefore may alter the level of CDD performed on a client and/or how it is conducted. out this CDD, depending on the specific circumstances of the situation.

11.8.2 When adverse information comes to light during the CDD process that cannot be satisfactorily addressed, the Company will not proceed to allow the relevant entity access to its services. Suspicions arising from information discovered during CDD should be reported to the CO as set forth above;

11.8.3 in all cases, regardless of any other CDD being done, the Company will obtain a report (including politically exposed person (“PEP”) checks and sanctions screening checks) on potential clients at an early stage, to identify whether any PEPs are involved and confirm that they would not be dealing with an individual or entity subject to UK, EU, US or UN sanctions. The Company will automatically reject any application where the client (or a beneficial owner of the client) is a PEP. Also, dealing with the issue of a financial penalty or helping someone to evade a financial penalty will generally involve the commission of a crime in the UK. As a result, if the report identifies a possible sanction match, it must be reviewed and approved by the CO before access can be granted;

11.8.4 some types of adverse information detailed in the report can be successfully addressed by making further inquiries to the client as part of the CDD process. For example, the Company may be able to address your concerns by confirming the client's source of wealth and that a legitimate source of funds will be used while using the Company's services;

11.8.5 a PEP roster review will be conducted quarterly to assess whether any current clients have become PEPs since first approved; and

11.8.6 if suspicions or concerns arise after access has been granted, the Company may nonetheless be under reporting obligations and will seek legal advice as appropriate. If, after the completion of an exchange through the Company's services, an alert is generated with adverse information related to one of the parties to the transaction, this alert must be brought to the CO without delay. Additionally, if an employee of the Company becomes aware of adverse media coverage or other information about a customer and/or a transaction that suggests there may be a money laundering problem, this should also be reported to the CO.

12. CUSTOMER CDD TIME

12.1 The Company is normally required to carry out due diligence when establishing the business relationship with the "client". However, you should also apply customer CDD measures at other appropriate times, taking a risk-based approach, particularly when it appears that the identity or ownership of the customer has changed, the relationship is not being used as intended, or it appears there is any risk of money laundering.

12.2 When the Company cannot apply CDD measures with the client, it must:

12.2.1 failing to establish a business relationship with the customer (if applicable);

12.2.2 not accept crypto assets from the client;

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

12.2.4 review any historical transactions to determine whether they presented a risk of involvement in financial crime; and

12.2.5 consider whether it is necessary to submit a report to the CO.

13. CONTINUOUS MONITORING OF THE COMMERCIAL RELATIONSHIP

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

13.2 In the normal course of business, the Company must be able to meet its obligation to conduct ongoing monitoring through a variety of compliance-related tasks, including data collection, filtering, record keeping, investigations and reports.

13.3 System functionalities include:

13.3.1 Daily checks of clients on their presence in the recognized "black lists" (for example, OFAC),

13.3.2 place users on denial of service and watch lists as appropriate, and

13.3.3 CDD information and document reviews (both spontaneous and periodic).

13.4 In addition to CCD reviews, the Company will engage in transaction monitoring activities. The Company will engage in the analysis of customer transaction patterns through data analytics and suspicious activity detection tools to assess whether particular transactions fall outside

of the general trends/risk profile that the Company has established (adding transfers by multiple data points) and/or the typical approach taken by specific customers.

13.5 Where a transaction presents itself as potentially a higher risk of financial crime based on previous monitoring, the Company will conduct additional appropriate investigations to determine whether financial crime is 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 clients wishing to make higher value trades must be subject to higher levels of CDD to reflect the increased risk of financial crime. Such thresholds work with cumulative and individual transaction evaluations to decrease the likelihood of smurfing by allowing transactions/customers to avoid additional CDD.

14. REGISTRY MANTENANCE

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

15. STAFF TRAINING

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

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

Content	• UK legal and regulatory regime in relation to financial crime • Specific infractions that can be committed by several employees within a company • The role of CO - Financial crime risks that the business is exposed to and how the Company seeks to mitigate and manage them. - The CDD and SAR procedures that the Company has in place, as well as broader obligations of employees with respect to the fight against financial crimes.

Recipients	- All directors, senior managers and employees - Consultants, secondes and similar workers will be determined on a case-by-case basis
Frequency	- All employees will receive training as part of their incorporation as employees. - At a defined point annually, all employees will complete a refresher training session.
Delivery method	- Desktop-based training slides, accessible at the discretion of employees
Confirmation	- Each time an employee receives training, they will be required to complete a mandatory assessment. They must pass this assessment to complete the training. - As part of an individual's annual performance review, it will be confirmed whether the individual completed financial crime training for that year. In addition, automated systems will identify to the CO those who have not completed the annual training within 1 month of the life of the training program.

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

16.1 Certain providers of professional services to the Company (particularly banks and other financial institutions, attorneys and agents) will be under AML obligations to carry out "know your customer" ('KYC') in the company as your customer. The key obligation placed on them by the 2017 MLRs is to confirm and verify the identity of their client, and they are typically required to do so before they can provide their services. Similarly, from time to time, professional services firms acting for other parties (for example, attorneys acting for an investor) will be required to perform KYC on the Company as one of the other parties to the agreements. (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 While a Companies House search will allow third parties to identify and verify key information such as the Company name, registration number and registered office address, the

2017 MLRs require companies to take a risk-based approach. This means that the Company may receive requests for additional information beyond what is contained in the public records, particularly when the transaction that triggers the requirement to carry out KYC on the Company presents indicators that there is a risk of money laundering. When this occurs, Company employees should ask the person making the request to explain and justify the basis for the request, and requests should then be considered on a case-by-case basis.

KYC PROCEDURES

This procedure describes the process by which the Company conducts customer due diligence on potential customers/merchants before they are given access to services. The same procedure is used for when an existing client changes his relationship with the Company (for example, if he begins to participate in a wider range of cryptocurrencies, or places significantly more funds on the platform). The purpose of this procedure is to help the Company develop business that is within its commercial risk appetite, but also to ensure that it meets its obligations with regard to customer due diligence arising under UK anti-money laundering legislation. of money and prevents its services from being used for the purposes of other financial crimes.

1. STEP 1 – IDENTIFY THE CUSTOMER AND DEFINE THE BUSINESS CASE

This stage is very important as it lays the groundwork on which the KYC procedure will be based. The process followed will vary depending on how the client is going to use the platform.

Merchants

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

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

1.2.1 In which country is the trader registered and what is the name of the trader?

1.2.2 Who are the directors, senior managers, shareholders, etc.?

1.2.3 What currencies would you like to receive your balance settlement?

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

1.2.5 What are they selling? What is the product/service and what industry does it belong to?

1.2.6 Who are your typical customers?

1.2.7 What are your target markets/main regions where customers come from?

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

1.2.9 How long have they been active?

1.2.10 Any additional information we should have?

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

Buyer Client

1.4 This stage consists of gathering as much information as is appropriate and possible from the client so that the Company is clear about who the client is, and so that this can be verified with documentary evidence.

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

1.5.1 Who is the actual customer (ie individual, company, trust, etc.)? What is the relationship of the person completing the identifying information to the entity?

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

1.5.3 If the entity is a person, what is their name, what is their date of birth, and where do they reside?

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

1.5.5 What crypto assets do they intend to trade?

1.5.6 What volume of transactions do they intend to carry out?

1.5.7 Which merchants do you intend to use?

1.5.8 Any additional information we should have?

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

0. STEP 2 – DOCUMENT COLLECTION

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

2.1.1 Constitution certificate

2.1.2 Memorandum and articles of association

2.1.3 Identities of Beneficial Owners (who may be subject to CDD as if they were the direct customer, depending on their risk profile)

2.1.4 Identities of the directors (or equivalent) (who may be subject to CDD as if they were the direct client, depending on their risk profile).

These documents must be certified by a lawyer, accountant, notary public or consular officer of the British Embassy or Consulate.

Merchants

2.2 In addition to the documents specified in paragraph 2.1, the Company will require documents issued by a regulated third party that provide proof of business address (eg, utility bills for the property/excerpts from company records).

2.3 The Company also requires all merchants, partners and any Non-Beneficial Owners of a merchant (as applicable) and, where the merchant is an incorporated company, at least two directors of the merchant to provide proof of verification that they meet each of the categories detailed in the table in paragraph 2.4

Buyer Client (and beneficial owners/directors where applicable)

2.4 A risk proportionality approach is adopted for the verification of purchasing clients. 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 it is implemented:

Required verfication	**The customers to which it applies**	**Accepted evidence**	**Collection method**
Name and date of birth	All customers	Identity document (for example, color copies of the passport)	Photograph taken by the client

Proof of residence	- Customers who intend to or have exceeded $100 in daily transactions on any given day. - Customers who intend to or have exceeded $1,000 in monthly transactions in any month. -Customers who present a moderate risk of financial crime	Utility bills or similar documents (not older than 3 months).	Photograph taken by the client
Biometric data	- Customers who intend to or have exceeded $1,000 in daily transactions on any given day. - Customers who intend to or have exceeded $5,000 in monthly transactions in any month. - Customers who present a higher risk of financial crime	Customer image	Photographic and facial scan captured through the client's device using the Company's application

2.5 As detailed above, depending on the particular level of transactions a customer engages in, they will be subject to additional levels of CDD due to the increased risk of financial crime that higher transaction volumes represent. The Company's systems automatically monitor a client's transaction volumes on an ongoing basis. When a customer reaches the transaction value limit of their current verification level, the Company's sy stems will immediately suspend that customer's ability to conduct further transactions until they complete the requirements for the next Verification level. The client will receive a notification advising them of the need to submit additional CDD information and the implications of not doing so. Upon the customer's

submission of the additional requested data, and the Company confirming that it meets its requirements for the additional CDD, the functionality of the customer will be restored.

0. REVISION

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

3.1.1 will review the adequacy of the documentary evidence received;

3.1.2 will compare the documentation received with the information collected from the client; and

3.1.3 will obtain a report including Politically Exposed Person ("PEP") checks and Sanctions checks and any other relevant persons named as part of the information collection.

3.2 Any discrepancies are highlighted and brought to the attention of the CO. Such action may lead to:

3.2.1 Identification of a potential money laundering/financial crime risk and subsequent activation of the relevant reporting processes;

3.2.2 identification that enhanced CDD or additional customer information is required, in which case the CO will be engaged and advice sought on additional verification steps to be undertaken; either

3.2.3 that the current documentation and information is deemed adequate, and therefore the standard CDD process will continue.

3.3 In addition, any documentation that is missing or does not conform to Company standards 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 carried out:

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, enter details on:

3.5.1 your identity (for example, full name, date of birth, address); and

3.5.2 documents collected for verification purposes (for example, passport number), on the integrated platform provided by the third-party service provider that the Company uses to assist with further identification/verification actions.

3.6 When this platform returns a result indicating:

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

3.6.2 the client appears on a PEP/sanction list,

The staff member must:

3.6.3 Review the results to confirm if this is a clear false-positive result or if there was a flaw in the initial data the staff member provided;

3.6.4 3.2

Reputation check

3.8 Google's checks are made on all companies and individuals that appear in company documents, as well as on the website. Keywords are used to find negative results like scam, fraud, etc.

3.8 During this check, the reviewer should consider:

3.8.1 For merchants - how long the brand or company has been in existence (and check that no results are found from before these dates) and if there is an indication of PEP participation. In addition, adverse means of any kind will also be considered.

3.8.2 For client buyers/owners/beneficial directors – if there is any indication that the client is or may be involved with PEP. In addition, adverse means of any kind will also be considered.

3.9 Negative results found are escalated and a decision is made if this prevents the Company from approaching the client and/or if it needs to be discussed with the client.

0. REVIEW AND APPROVAL

4.1 It is the Company's policy not to provide access to services, accept assets from, or carry out any transaction of any kind with respect to, any client until (i) that client has provided documentation in compliance with the standards set forth above, (ii)) the identity of the client has been verified to an appropriate level in accordance with its risk profile, and (iii) the client has accepted the relevant terms of business set out above.

16.2.1 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 profile customer's original risk has changed), and the customer is unable to provide documentation that meets the required standard, the Company will terminate its existing business relationship and consider whether a disclosure to the authorities is required.