# Anti-Money Laundering Policy

**CR MARKETS, LLC.**

**ANTI-MONEY LAUNDERING POLICY**

**1.** CRM ANTI-MONEY LAUNDERING ("AML") POLICY

Money laundering – the process of converting funds, received from illegal activities (such as fraud, corruption, terrorism, etc.), into other funds or investments that look legitimate to hide or distort the real source of funds. The process of money laundering can be divided into three sequential stages:

- Placement. At this stage funds are converted into financial instruments, such as checks, bank accounts, and money transfers, or can be used for purchasing high-value goods that can be resold. They can also be physically deposited into banks and non-bank institutions (e.g., currency exchangers). To avoid suspicion by the company, the launderer may as well make several deposits instead of depositing the whole sum at once, this form of placement is called smurfing.

- Layering. Funds are transferred or moved to other accounts and other financial instruments. It is performed to disguise the origin and disrupt the indication of the entity that made the multiple financial transactions. Moving funds around and changing in their form makes it complicated to trace the money being laundered.

- Integration. Funds get back into circulation as legitimate to purchase goods and services.

**2.** POLICY STATEMENT AND PRINCIPLES

CR Markets, LLC. (“CRM”) has adopted an Anti-Money Laundering (AML) compliance policy ("Policy") in compliance with The Financial Intelligence and Anti-Money Laundering Act 2002 (FIAMLA 2002), the Prevention of Corruption Act 2002 (POCA 2002) and the Prevention of Terrorism Act 2002 (POTA 2002).

**3.** SCOPE OF POLICY

This policy applies to all CRM officers, employees, appointed producers and products and services offered by CRM. Every business unit and location within CRM will cooperate to create a cohesive effort in the fight against money laundering. Each business unit and location has implemented risk- based procedures in an effort to prevent, detect and report transactions as required under the FIAMLA. All efforts implemented will be documented and retained in accordance with the FIAMLA. The AML Compliance Committee is responsible for initiating Suspicious Activity Reports ("SARs") or other required reporting to the appropriate law enforcement or regulatory agencies. Any contacts by law enforcement or regulatory agencies related to the Policy shall be directed to the AML Compliance Committee.

**4.** POLICY

Money laundering is the process of concealing the real source of criminally derived incomes such as fraud, theft, drug trafficking or any other crimes. Money laundering could also include using legally derived funds such as financial products and transactions to finance terrorism or other money laundering schemes. CRM strictly prohibits and actively prevents the occurrence of money laundering and any activity that facilitates

money laundering or the funding of terrorist or criminal activities. CRM is committed to AML compliance in accordance with applicable law and requires its officers, employees and appointed producers to adhere to these standards in preventing the use of its products and services for money laundering purposes.

Generally, money laundering consists of three stages. Firstly, cash enters the financial system at the "placement" stage, where the cash generated from criminal activities is converted into monetary instruments, such as money orders or traveller's checks, or deposited into accounts at financial institutions. At the "layering" stage, the funds are transferred or moved into other accounts or other financial institutions to further separate the money from its criminal origin. At the "integration" stage, the funds are reintroduced into the economy and used to purchase legitimate assets or to fund other criminal activities or legitimate businesses. Terrorist financing may not involve the proceeds of criminal conduct, but rather an attempt to conceal the origin or intended use of the funds, which will later be used for criminal purposes.

## **5.** AML COMPLIANCE COMMITTEE

The AML Compliance Committee comprises of the General Counsel; Chief Compliance Officer, CRM; Deputy Compliance Officer, CRM; Assistant Vice President-Internal Audit, and Corporate Attorney shall be wholly responsibility for the Policy. The Chief Compliance Officer also holds the title Chief AML Officer and has the authority to sign as such. The responsibilities of the AML Compliance Committee with regards to the Policy includes but are not limited to the designing, executing and the updating of the Policy as required. This involves the dissemination of information to officers, employees and appointed producers of CRM; monitoring the compliance of CRM operating units and appointed producers, maintaining necessary and appropriate records, filing of SARs when warranted; training of officers, employees and appointed producers and independent testing of the operation of the Policy. Each CRM business unit shall appoint a person in charge to liaise directly with the AML Compliance Committee to assist the Committee with investigations, monitoring and other required activities.

## **6.** CUSTOMER IDENTIFICATION PROGRAM

CRM has implemented a Customer Identification Program (CIP). CRM will notify customers prior to gathering customers' identification information. This includes collecting, recording and verifying specific minimum customer identification information of each customer and finally comparing customer identification information with OFAC.

## **7.** NOTICE TO CUSTOMERS

CRM will provide notice to customers that it is requesting information from them to verify their identities, as required by applicable law.

## **8.** VERIFYING INFORMATION

CRM will make sure that it is dealing with a real person or legal entity. CRM also performs all the required measures in accordance with applicable law and regulations, issued by monetary authorities. The AML policy is being fulfilled within CRM by means of the following: know your customer policy and due diligence monitoring of client activity record keeping. Because of the company's commitment to the AML and KYC policies, each client of the company has to finish a verification procedure. Before CRM starts any

cooperation with the client, the company ensures that satisfactory evidence is produced or such other measures that will produce satisfactory evidence of the identity of any customer or counterparty are taken. The company as well applies heightened scrutiny to clients, who are residents of other countries, identified by credible sources as countries, having inadequate AML standards or that may represent a high risk for crime and corruption and to beneficial owners who resides in and whose funds are sourced from named countries.

Individual clients

During the process of registration, each client provides personal information, specifically: full name; date of birth; origin; complete address, including phone number and city code. A client sends the following documents (in case the documents are written in non-Latin characters: to avoid any delays in the verification process, it is necessary to provide a notarized translation of the document in English) because of the requirements of KYC and to confirm the indicated information:

- A high-resolution copy of the first page of local or international passport, where the photo and the signature are clearly seen, or a copy of driver's license with the same requirements. The indicated documents must be valid at least 6 months from the filing date.

- A high-resolution copy of a receipt of utility services payment or bank statement, containing the full client's name and the actual place of residence. These documents should not be older than 3 months from the date of filing.

Corporate clients

In case the applicant company is listed on a recognized or approved stock exchange or when there is independent evidence to show that the applicant is a wholly owned subsidiary or a subsidiary under the control of such a company, no further steps to verify identity will normally be required. In case the company is unquoted and none of the principal directors or shareholders already has an account with CRM, the official provides the following documents because of the requirements of KYC:

- a high-resolution copy of the certificate of incorporation/certificate;

- an extract from the Commercial Register, or equivalent document, evidencing the registration of corporate acts and amendments;

- names and addresses of all officers, directors and beneficial owners of the corporate entity;

- a high-resolution copy of Memorandum and Articles of Association or equivalent documents duly recorded with the competent registry;

- evidence of the company’s registered address and the list of shareholders and directors;

- description and nature of business (including the date of commencement of the business, products or services provided; and the location of principal business).

This procedure is performed to establish the identity of the client and to help CRM know/understand the clients and their financial dealings to be able to provide the best services of online trading.

Depending on the risk and to the extent reasonable and practicable, CRM will ensure that it has a reasonable belief of the true identity of its customers. In verifying customer identity, appointed producers shall review photo identification. CRM shall not attempt to determine whether the document that the customer has provided for identification has been validly issued. For verification purposes, CRM shall rely on a government issued identification to establish a customer's identity. CRM, however, will analyze the information provided to ensure that there are no logical inconsistencies in the information obtained. CRM will document its verification, including all identifying information provided by the customer, the methods used and results of the verification, including but not limited to sign-off by the appointed producer of matching photo identification.

## **9.** CUSTOMERS WHO REFUSE TO PROVIDE INFORMATION

If a customer either refuses to provide the information described above when requested, or appears to have deliberately provided misleading information, the appointed agent shall notify their New Business team. The CRM New Business team will decline the application and notify the AML Compliance Committee.

## **10.** CHECKING THE OFFICE OF FOREIGN ASSETS CONTROL ("OFAC") LIST

For all (1) new applications received and on a continuous basis, (2) disbursements (3) new producers appointed or (4) new employees, CRM will check to ensure that a person or entity does not appear on Treasury's OFAC "Specifically Designated Nationals and Blocked Persons" List (SDN List) and is not from, or engaging in transactions with people or entities from, embargoed countries and regions listed on the OFAC Web Site.

To ensure a speedy and accurate check, CRM shall contract with World-Check. CRM will also review existing policy holders, producers and employees against these lists on a periodic basis. We will then document and retain the frequency of these reviews. If there is a match to the SDN List or other OFAC List, the business unit will conduct a review of the circumstances where such

match has been identified as stated herein. If the business unit is incapable of confirming that the match is a false positive, the AML Committee shall be notified.

## **11.** MONITORING AND REPORTING

In addition to gathering information from the clients, CRM continues to monitor the activity of every client to identify and prevent any suspicious transactions. A suspicious transaction is known as a transaction that is inconsistent with the client's legitimate business or the usual client's transaction history known from client activity monitoring. CRM has implemented the system of monitoring the named transactions (both automatic and, if needed, manual) to prevent using the company's services by criminals.

Transaction based monitoring will occur within the appropriate business units of CRM. Monitoring of specific transactions will include but is not limited to transactions aggregating $5,000 or more and those with respect to which CRM has a reason to suspect suspicious activity. All reports will be documented and retained in

accordance with the FIAMLA requirements.

All the clients' operations to deposit and withdraw funds have the following requirements: In case of bank transfer or transfer from a bank card, the name, indicated during the registration must match the name of the owner of the account/bank card. Withdrawing funds from the trading account via the method, which is different from the depositing method, is possible solely after withdrawing the sum, which is equal to the sum of client's deposits via the method and to the same account used for depositing. If the account was credited in the way that cannot be used for funds withdrawal, the funds may be withdrawn to a bank account of the client or any other way may be used, as agreed with the Company with the help of which the Company is able to prove the identity of the account owner.

If the account has been credited with funds through various payment systems, funds withdrawal shall be made on a pro rata basis commensurate to the size of each deposit. In case of depositing via Visa/MasterCard, Wire Transfer, ePayments, the withdrawal of funds, which exceed the sum of the client's deposits, is possible via any of the following methods: Visa/MasterCard, Wire Transfer, ePayments. In case of depositing via another method, the withdrawal of funds that exceed the sum of the client's deposits, is possible via any available method, by the client's choice.

## **12.** SUSPICIOUS ACTIVITY

“Red flags” are commonly used to refer to signs of suspicious activity that suggest money laundering.

Whenever a red flag is detected, additional due diligence will be performed before proceeding with the transaction. If a reasonable explanation is not provided, the suspicious activity shall be reported to the AML Compliance Committee. Examples of red flags are:

- The customer displays unusual concern about the firm's compliance with government reporting requirements and the firm's AML policies, especially regarding his or her identity, type of business and assets, or is reluctant or refuses to disclose any information

concerning business activities, or furnishes unusual or suspect identification or business documents.

- The information provided by the customer that identifies a legitimate source for funds is false, misleading, or significantly incorrect.

- Upon request, the customer refuses to identify or fails to indicate any legitimate source for his or her funds and other assets.

- The customer has difficulty describing the nature of his or her business or lacks general knowledge of his or her industry.

- The customer wishes to engage in transactions that lack business sense or superficial investment strategy, or are inconsistent with the customer's indicated business strategy.

- The customer (or a person publicly associated with the customer) has a questionable background or is the subject of news reports indicating possible criminal, civil, or regulatory violations.

- The customer displays a lack of concern regarding risks, commissions, or other transaction costs.

- The customer appears to be acting as an agent for an undisclosed principal, but refuses or is reluctant, without valid commercial reasons, to provide information or is otherwise ambiguous regarding that person or entity.

- The customer attempts to make frequent or large deposits of currency, insists on dealing only in cash equivalents, or asks for exemptions from the firm's policies relating to the deposit of cash and cash equivalents.

- The customer engages in transactions involving cash or cash equivalents or other monetary instruments that appear to be structured to avoid the $10,000 government reporting requirements, especially if the cash or monetary instruments are in an amount just below reporting or recording thresholds.

- For no apparent reason, the customer has multiple accounts under a single name or multiple names, with a large number of inter-account or third-party transfers.

- The customer is from, or has accounts in, a country identified as a non-cooperative country or territory by the Financial Action Task Force.

- The customer's account shows numerous currency or cashier’s check transactions aggregating to significant sums.

- The customer's account has unexplained or sudden extensive wire activity, especially in accounts that had little or no previous activity.

- The customer's account has a large number of wire transfers to unrelated third parties inconsistent with the customer's legitimate business purpose.

- The customer's account has wire transfers that have no apparent business purpose to or from a country identified as money laundering risk or a bank secrecy haven.

- The customer's account indicates large or frequent wire transfers, immediately withdrawn by check or debit card without any apparent business purpose.

- The customer makes a funds deposit followed by an immediate request that the money be wired out or transferred to a third party, or to another firm, without any apparent business purpose.

- The customer makes a funds deposit for the purpose of purchasing a long-term investment followed shortly thereafter by a request to liquidate the position and transfer of the proceeds out of the account.

- The customer engages in excessive journal entries between unrelated accounts without any apparent business purpose.

- The customer's account shows an unexplained high level of account activity with very low levels of securities transactions.

- The customer requests that a transaction be processed in such a manner to avoid the firm's normal documentation requirements.

**13.** INVESTIGATION

Upon notification to the AML Compliance Committee of a match to the OFAC SDN List or possible suspicious activity, an investigation will be commenced to determine if a report should be made to appropriate law enforcement or regulatory agencies. The investigation will include, but not necessarily be limited to, review of all available information, such as payment history, birth dates, and address. If the results of the investigation warrant, a recommendation will be made to the AML Compliance Committee to file a blocked assets and/or a SAR with the appropriate law enforcement or regulatory agency. The AML Compliance Committee is responsible for any notice or filing with law enforcement or regulatory agency. Investigation results will not be disclosed or discussed with anyone other than those who have a legitimate need to know. Under no circumstances shall any officer, employee or appointed agent disclose or discuss any AML concern, investigation, notice or SAR filing with the person or persons subject of such, or any other person, including members of the officer's, employee's or appointed agent's family.

**14.** RECORDKEEPING

The AML Compliance Committee will be responsible to ensure that AML records are maintained properly and that SARs and Blocked Property Reports are filed as required. CRM will maintain AML records for at least five years.

**15.** TRAINING

CRM shall provide general AML training to its officers, employees and appointed producers to ensure awareness of requirements under the FIAMLA. The training will include, at a minimum: how to identify red flags and signs of money laundering; what roles the officers, employees and appointed producers have in the CRM compliance efforts and how to perform such duties and responsibilities; what to do once a red flag or suspicious activity is detected; CRM record retention policy; and the disciplinary consequences for non-compliance with the Act and this Policy. In addition, each affected area will provide enhanced training in accordance with the procedures developed in each area for officers and employees reasonably expected to handle money, requests, or processing that may bring them into contact with information designated above. Training will be conducted on an annual basis. The CRM AML Compliance Committee will determine the ongoing training requirements and ensure written procedures are updated to reflect any changes required in such training. CRM will maintain records to document that training has occurred.

**16.** TESTING OF THE POLICY

The testing of the Policy will be conducted by an outside independent third party annually. Any findings will be reported to the AML Compliance Committee, SFG Audit Committee and Senior Management for appropriate action.

**17.** ADMINISTRATION

The AML Compliance Committee is responsible for the administration, revision, interpretation, and application of this Policy. The Policy will be reviewed annually and revised as needed.

Updated: March 22, 2022.

## SPECIFICATION

1. Subject to the terms of this Agreement, the Service Provider shall provide to the Customer the following Services, including, where applicable, conducting Checks as described in the tables below and receiving Reports containing the results of such Checks:

**KYC:**

| Service Name | Description |
|---|---|
| Email verification | Verification of email addresses to ensure their validity and that they belong to a real person. |
| Phone verification | Verification of phone numbers to ensure their validity and that they belong to a real person. |
| Identity Document Verification | Determination of whether a document is authentic, legitimate, and free of forgery or alteration. |
| Automated data extraction (Basic five fields) | Automatic extraction of data from identity documents for further processing. By default, five fields are extracted:<br><br>- Full name,<br>- Date of birth,<br>- Document number,<br>- Issue date,<br>- Expiration date. |
| Automated data extraction (Additional fields) | Extraction of custom fields, depending on regulatory requirements and/or business needs. These may include gender, tax number, address, additional number, etc. |
| Ongoing Document Monitoring | Daily re-check of the validity of identity documents previously submitted by a given user, based on their expiry date. This includes sending automated requests for replacements if documents expire. |
| Liveness check and Face Match | Biometric analysis of a person's facial movements that is compared with photographs on submitted documents. This is to ensure that a person is truly present and that their documents belong to them. |

| | |
|---|---|
| Known face search | Determintion of whether a person's face is duplicated or present on blacklists. |

| | |
|---|---|
| AML Screening: International Sanctions, PEPs, Watchlists and Adverse Media | Determination of a natural person's presence or non-presence on global sanctions lists, PEP lists, watchlists, blacklists, or adverse media (OFAC, UN, HMT, EU, DFT etc.).<br><br>This check is automated and does not make any final decisions on whether to onboard a given person (such decisions are made by the Customer at their own discretion). The results of this Check are solely based on potential matches between the user's personal data and the data contained in databases available to the Service Provider. |
| Ongoing AML monitoring | Daily re-check of the customer database against AML watchlists (sanctions, PEPs, adverse media, etc). Once AML screening is initiated, ongoing monitoring is included for one year. |
| Proof of Address Check | Verification of addresses and residency through analysis of the following documents:<br><br>- Driving licenses bearing residential address;<br>- Tax bills;<br>- Utility bills;<br>- Voter rolls;<br>- Bank statements;<br>- Other documents commonly accepted as proof of address. |

**Other Services:**

| Service Name | Description |
|---|---|
| Customer Accounts | Maintenance of one or more active accounts in the System (dashboard) for the purposes of compliance, data managment, customer support, etc. An account is considered "active" if it is logged into at least once during a given reporting (billing) period. |
| Questionnaire | Questionnaire customization that enables gathering specific information from Applicants as necessitated by other Checks or by the Customer's risk-assessment policies. |
| SMS notification service | SMS notification of users when necessary. The SMS notification service is integral to other services, such as "Switch to mobile via SMS link" and "Phone verification". Alternatively, your Twilio accounts may be used. |
| White Label | Optional customization of branded elements, including domains, email addresses, and verification links. |
| Web SDK and Mobile SDK | The default type of integration. |
| API | Integration via API instead of Web SDK or Mobile SDK. |

| | |
|---|---|
| Additional services | - Reporting module;<br>- Basic analytics and statistics;<br>- External integrations with Slack, Telegram, Email, Twilio, etc.;<br>- SAML/SSO;<br>- Switch to mobile via SMS link;<br>- Email notification service. |

2. For clarity, a Check is deemed completed when a given Applicant is assigned a temporary or final “Rejected”, “Approved”, or "Resubmission requested" status in the System. If any Check from the table above is reiterated in respect of the same Applicant later than one calendar month from the moment when the first such Check was completed or, irrespectively of the timing, by the Customer or at the Customer's request, such reiteration shall be considered a new Check and, therefore, fully charged for in accordance with Annex 2 to this Agreement.

3. The Customer may choose all or some of the Services listed in the tables above; in the latter case, the Customer shall deliver to the Service Provider, prior to the Commencement Date, written notice specifying the chosen Services. Check marks left by the Customer next to the names of relevant Services in Annex 2 to this Agreement shall be considered an equal alternative to such notice. The list of the chosen Services shall only be amended based on written notice subsequently delivered by the Customer to the Service Provider.

# SERVICE PROVIDING TERMS AND CONDITIONS

## 1. DEFINITIONS AND INTERPRETATIONS

1.1 In this Agreement, unless the context otherwise requires, the following definitions shall apply:

**API** means a set of functions and procedures that facilitate submission of applications for access to the features or data of the System.

**Applicant** means the end user (whether natural person or legal entity) providing documents, images, and other input data in respect of which the Service Provider performs Checks and other Services.

**Business Purpose** means the permitted purpose for which the Customer may use the System and the Services as detailed in the Cover Sheet. For clarity, the Business Purpose does not include determining an Applicant's eligibility for credit or insurance for personal, family or household purposes, employment or a government license or benefit.

**Check** means a subcategory of the Services consisting of analysis of documents, images, and other input data submitted by a given Applicant carried out in order to verify the Applicant's identity.

**Commencement Date** means the day this Agreement becomes effective as set out in the Cover Sheet.

**Confidential Information** means information disclosed by (or on behalf of) one party to the other party in connection with or in anticipation of this Agreement (including the content of this Agreement) that is marked as confidential or, from its nature, content or the circumstances in which it is disclosed, might reasonably be supposed to be confidential. It does not include information (i) that the recipient already knew, (ii) that becomes public through no fault of the recipient, (iii) that was independently developed by the recipient or (iv) that was lawfully given to the recipient by a third party.

**Fees** means the charges payable by the Customer to the Service Provider in accordance with this Agreement and, specifically, Annex 2 hereof.

**Good Industry Practice** means, in relation to any undertaking and any circumstances, the exercise of skill, diligence, prudence, foresight and judgement and any expenditure that would reasonably be expected from a skilled person engaged in the same type of undertaking under the same or similar circumstances.

**Intellectual Property Rights** means all patents, rights to inventions, utility models, copyright and related rights, trademarks, service marks, trade, business and domain names, rights in trade dress or get-up, rights in goodwill or to sue for passing off, unfair competition rights, rights in designs, rights in computer software, database rights, topography rights, moral rights, rights in Confidential Information (including know-how and trade secrets) and any other intellectual property rights, in each case whether registered or unregistered and including all applications for and renewals or extensions of such rights, and all similar or equivalent rights or forms of protection in any part of the world.

**Malicious Code** means viruses, worms, time bombs, Trojan horses and other similar malware, files, scripts, agents or programs.

**Customer System** means any information technology system or systems owned or operated by Customer (if any) which receives any data from the Service Provider in accordance with this Agreement, including Customer's data processing facilities, data files and documents needed for processing.

**Customer User** means any member of the Customer's personnel authorised by the Customer to access and/or use the System (in its entirety or in part) under their own unique identifier provided by the Service Provider.

**Reports** means documents generated in the Dashboard and containing summaries of the Checks performed in respect of each given Applicant and of their results.

**Security Feature** means any key, PIN, password, token, smartcard, etc.

**Support** means the technical support to be provided by the Service Provider, including maintaining the System accurate, up-to-date, in good working order, and free from Malicious Code, and to restore it to normal operational conditions if unavailable.

**System** means a set of computer programs and databases owned and operated by the Service Provider in order to render the services described in Schedule 1 (the **"Services"**). The System includes an interactive software tool facilitating the communication between the Service Provider and the Customer and ensuring management and processing of requests for verification submitted by the Customer or by Applicants (the "**Dashboard**").

1.2 Where the expressions "include(s)", "including" or "in particular" are used in this Agreement, the list of words following them shall not be considered exhaustive.

1.3 References to clauses are to the respective clauses of this Agreement.

1.4 A reference to a party includes its successors and permitted assigns.

**2. CONNECTION OF THE SYSTEM AND PROVISION OF THE SERVICES**

2.1 The Service Provider shall enable connection to the System on and from the Commencement Date and shall promptly provide the Services in accordance with the specifications set out in Schedule 1 (if any) and supply any new releases to the Customer.

2.2 Each party shall bear its own costs of establishing that connectivity provided that the Service Provider must provide the Customer with all reasonable assistance and information to achieve the connectivity in a timely manner.

2.3 The Service Provider shall, for the duration of the Term, provide the Services to Customer in accordance with Good Industry Practice, Schedule 1 and the SLA.

2.4. The Customer acknowledges that for any reason, at any time, and without prior notice, the Service Provider may issue updates to the provided Services / the System, and agrees to use commercially reasonable efforts to install such updates in a timely manner. Failure of the Customer to update all versions

of the Service Provider's Services / the System within 60 days of written upgrade notification from the Service Provider shall be considered a material breach in accordance with clause 8.3 of this Agreement. The Service Provider shall send written upgrade notifications via email address or through the System notification mechanism. The Service Provider shall not be in any way liable for the incorrect operation of the System due to the failure of the Customer to perform the obligation to update the Services / the System.

**3. INTELLECTUAL PROPERTY RIGHTS - OWNERSHIP AND PROTECTION**

3.1 The Customer acknowledges and agrees that all Intellectual Property Rights in the System are the property of the Service Provider or its Service Providers (as the case may be) and the Customer shall have no rights in or to the System other than the right to use them in accordance with the express terms of this Agreement.

**4. CHARGES**

4.1 For provision of the Services and use of the System, including receipt of any new releases, Support, or maintenance as per the terms of this Agreement, the Customer shall pay the Service Provider charges as detailed in Annex 2 to this Agreement.

4.2 Unless it is stated otherwise in Annex 2 to this Agreement, the Service Provider shall invoice the Customer no later than the 10th day of the month following the reporting period (meaning the period in which the chargeable Services were actually provided), and the Customer shall pay the correct invoices within 10 business days of receipt from the Service Provider.

4.3. The Service Provider shall have the right to suspend access to the Services until the Customer makes the due payment as required under clauses 4.1-4.2 and Annex 2 to this Agreement. Additionally, the Service Provider shall be entitled to a penalty in the amount of 1% of the due payment per each day of such delay.

**5. CONFIDENTIALITY AND DATA PROTECTION**

5.1 The recipient of any Confidential Information will not disclose that Confidential Information, except to employees and/or professional advisors who need to know it and who have agreed in writing (or in the case of professional advisors are otherwise bound) to keep such information confidential. The recipient will ensure that those people and entities: (a) use such Confidential Information only to exercise rights and fulfil obligations under this Agreement; and (b) keep such Confidential Information confidential. The recipient may also disclose Confidential Information when required by law after giving reasonable notice to the discloser, such notice to be sufficient to give the discloser the opportunity to seek confidential treatment, a protective order or similar remedies or relief prior to disclosure.

5.2 The Service Provider shall guarantee the level of protection of personal data that it received at the level required by the law applicable to such personal data (including the EU General Data Protection Regulation where applicable). The regime of personal data protection is set out in Annex 3 to this Agreement.

5.3 The Service Provider shall, subject to Clause 5.2, upon the relevant request of the Customer, transfer free of charge to the Customer without delay all the information collected within and in relation to offering its Services under this Agreement (including but not limited to various KYC and AML related information about

the users). Service Provider shall transfer the information in a structured and organised manner (structured by the users, type of information etc.) to enable the Customer the subsequent use of the information. Upon the request for the transfer of information Customer and Service Provider shall agree upon the method of the transfer to achieve the goal set forth in this clause.

**6. SECURITY FEATURES AND SUPPORT**

6.1 Where the Service Provider uses Security Features in relation to the System, the Customer shall use reasonable endeavours to keep the Security Features confidential and not share the Security Features other than with the Customer Users and/or Applicants.

6.2 The Service Provider shall provide Support in accordance with its normal business practices and Good Industry Practice.

**7. LIABILITY. LIMITATION OF LIABILITY**

7.1 Neither party excludes or limits liability to the other party for: (a) fraud or fraudulent misrepresentation; (b) death or personal injury caused by negligence; (c) a breach of any terms implied by section 12 of the Sale of Goods Act 1979 or section 2 of the Supply of Goods and Services Act 1982; (d) any indemnities under this Agreement or (e) any matter for which it would be unlawful for the parties to exclude liability.

7.2 Subject to clause 7.1, each party shall not in any circumstances be liable whether in contract, tort (including for negligence and breach of statutory duty howsoever arising), misrepresentation (whether innocent or negligent), restitution or otherwise, for: (a) any loss of profits; (b) any loss or corruption of data or information, except loss or corruption of data caused by a breach of this Agreement by either party.

7.3 Subject to clause 7.1, each party's total aggregate liability in contract, tort (including negligence and breach of statutory duty howsoever arising), misrepresentation (whether innocent or negligent), restitution or otherwise, arising in connection with the performance or contemplated performance of this Agreement or any collateral contract shall in all circumstances be limited to 100% of the total Charges paid by the Customer to the Service Provider during the 3-month period immediately before the date on which the cause of action first arose.

**8. TERM AND TERMINATION**

8.1 This Agreement shall commence on the Commencement Date. Unless terminated earlier in accordance with clauses 8.2 or 8.3 this Agreement shall continue for the duration of the Term as specified in the Cover Sheet.

8.2 The Customer may terminate this Agreement at any time for convenience by giving the Service Provider no less than 30 days prior written notice.

8.3 Without prejudice to any rights that have accrued under this Agreement or any of its rights or remedies, either party may terminate this Agreement with immediate effect by giving written notice to the other party if:

(a) the other party is in material breach of this Agreement where the breach is incapable of remedy; or (b) the other party is in material breach of this Agreement where the breach is capable of remedy and fails to remedy that breach within fourteen (14) days after receiving written notice of such breach; or (c) the other party enters into an arrangement or composition with or for the benefit of its creditors, goes into administration, receivership or administrative receivership, is declared bankrupt or insolvent or is dissolved or otherwise ceases to carry on business; or (d) any analogous event happens to the other party in any jurisdiction in which it is incorporated or resident or in which it carries on business or has assets.

8.4 Any provision of this Agreement that expressly or by implication is intended to come into or continue in force on or after termination of this Agreement shall remain in full force and effect. Termination of this Agreement, for any reason, shall not affect the accrued rights, remedies, obligations or liabilities of the parties existing at termination.

8.5 On any termination of this Agreement for any reason or expiry of the Term, each party shall as soon as reasonably practicable return or destroy (as directed in writing by the other party) all data, information, software, and other materials provided to it by the other party in connection with this Agreement including all materials containing or based on the other party's Confidential Information.

**9. GENERAL**

9.1 Neither party will be liable for any delay or non-performance of its obligations under this Agreement to the extent that such delay or non-performance is a result of any condition beyond its reasonable control, including but not limited to, governmental action, acts of terrorism, earthquake, fire, flood or other acts of God, labour conditions, power failures, and Internet disturbances.

9.2 No variation of this Agreement shall be valid unless it is in writing and signed by or on behalf of each of the parties. Failure or delay in exercising any right or remedy under this Agreement shall not constitute a waiver of such (or any other) right or remedy.

9.3 If any provision of this Agreement (or part of any provision) is found by any court or other authority of competent jurisdiction to be invalid, illegal or unenforceable, that provision or part-provision shall, to the extent required, be deemed not to form part of the Agreement; and (a) the parties shall immediately commence good faith negotiations to remedy such invalidity; and (b) the validity and enforceability of the other provisions of the Agreement as applicable shall not be affected.

9.4 This Agreement constitutes the whole agreement between the parties and supersedes any previous arrangement, understanding or agreement between them relating to the subject matter of this Agreement. Each party acknowledges that in entering into this Agreement it has not relied upon any oral or written statements, collateral or other warranties, assurances, representations or undertakings which were made by or on behalf of the other party in relation to the subject-matter of this Agreement at any time before its signature other than those which are set out in this Agreement.

9.5 Except as expressly stated otherwise, nothing in this Agreement shall create or confer any rights or other benefits in favour of any person other than the parties to this Agreement. Except as expressly stated otherwise, nothing in this Agreement shall create an agency, partnership or joint venture of any kind

between the parties. Neither party shall have authority to act in the name of or on behalf of the other, or to enter into any commitment or make any representation or warranty or otherwise bind the other in any way.

9.6 Neither party may assign any of its rights or obligations under this Agreement without the prior written consent of the other such consent not to be unreasonably withheld save that either party can assign to an acquirer of all or substantially all of the assets of a party without the consent of the other.

9.7 Each party is only permitted to make public announcements and/or publish written materials concerning the other party and/or the existence and nature of the business relationship between the parties if the other party has given its prior written consent to the content of such an announcement or the text of such a written material, except as required by law, any governmental or regulatory authority (including, without limitation, any relevant securities exchange), any court or other authority of competent jurisdiction. However, notwithstanding this and clause 3 of this Agreement, each party may freely use the other party's trademarks (including logos) for promotional purposes for the sole purpose of publicly identifying such other party as its counterparty.

9.8 All notices must be in English, in writing, addressed to the other party's primary contact and sent to their then current postal address or email address or other address as either party has notified the other in accordance with this clause. All notices shall be deemed to have been given on receipt as verified by written or automated receipt or electronic log (as applicable).

9.9 The parties shall: (i) comply with all applicable laws, statutes and regulations relating to anti-bribery and anti-corruption including to the Bribery Act 2010 (Relevant Requirements); (ii) not engage in any activity, practice or conduct which would constitute an offence under sections 1, 2 or 6 of the Bribery Act 2010 if such activity, practice or conduct had been carried out in the UK; (iii) promptly report to the other party any request or demand for any undue financial or other advantage of any kind received by it in connection with the performance of this Agreement.

9.10 This Agreement and all disputes and claims arising out of or in connection with it are governed by English law. With the sole exception of any application for injunctive relief, the parties irrevocably agree that the courts of England have exclusive jurisdiction to settle any dispute or claim (whether contractual or non-contractual) arising out of or in connection with this Agreement (including their subject matter or formation).